User Guide

hp StorageWorks HA-Fabric Manager

Product Version: FW v06.xx/HAFM SW v08.02.00

Fourth Edition (July 2004)

Part Number: AA–RS2CE–TE

This guide describes the HP StorageWorks High Availability Fabric Manager (HAFM) and its features. It tells you how to use the HAFM to monitor, configure, and manage the Fibre Channel in which managed products operate. This guide also covers Fabric zoning, HAFM appliance administration, and HAFM logs.

HA-Fabric Manager User Guide
Fourth Edition (July 2004)
Part Number: AA–RS2CE–TE

Contents

Figures

Tables

About This Guide

This user guide provides information to help you:

- Use the High Availability Fabric Manager (HAFM) to monitor, configure, and manage the Fibre Channel in which managed products operate.
- Manage Fabric zoning and HAFM logs.

"About this Guide" topics include:

Overview

This section covers the following topics:

Intended Audience

This book is intended for use by data center administrators, LAN administrators, operations personnel, and customer support personnel who:

- Administer user access to the *HAFM* application.
- Monitor and manage product operation.

Related Documentation

For a list of corresponding documentation, refer to the Related Documents section of the Release Notes that came with the product.

For the latest information, documentation, and firmware releases, please visit the following StorageWorks web site:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Association web site, located at http://www.fibrechannel.org.

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document Conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, refer to the HP web site for locations and telephone numbers: http://www.hp.com.

Introduction and General Information

1

This chapter presents an overview of the High Availability Fabric Manager (HAFM). It includes:

The Life Cycle of a SAN

The *HAFM* application enables you to proceed through the managed life cycle of the SAN with confidence.

Figure 1: The Life Cycle of a SAN

The first stage of a SAN's life cycle is to Plan the SAN. Use paper and pen or a software application to plan the SAN.

The second stage of the life cycle is to Discover the SAN. The *HAFM* application establishes contact with many SAN devices, gathers embedded information, and then depicts it in the Physical Map, or topology. The application discovers the devices attached to the SAN and presents an intuitive visual map of devices and their connections.

The third stage of the life cycle is to Configure the SAN, during which you should configure SAN devices and fabrics.

The final and longest stage of the life cycle is to Monitor the SAN. The application generates events and messages about product and property status. The user interface features an animated display of the data flow and error rates over the entire topology. The application's self-monitoring, event-logging, and event notification features allow you to stay informed about the state of the SAN.

At any point, a discovered SAN can be used as a starting point to plan a new SAN, completing the life cycle.

Product Licensing Overview

License and feature keys are unique strings of alphanumeric characters that verify ownership of software and additional software modules and features that you can purchase.

License Keys

License keys verify ownership of the license to use software application and optional features and modules. The use of license keys is new for this release. Depending on your upgrade situation, you may be prompted to enter the license key and software serial number the first time that you initialize the application to verify your software license. As you purchase additional software modules, you must enter license keys into the License Key dialog box (**Help** menu, **License** option). For details on acquiring license keys, see "Managing Users" on page 57.

If you order additional software modules after your initial purchase of the application, you will need to enter your original serial number, as well as a license key into the License Key dialog box (**Help** menu, **License** option). The software license key allows you to access the application and all optional software features or modules that you have purchased. Your ship kit documents provide a new software entitlement request certificate for HAFM, based on the number of ports. To obtain a license key, follow instructions provided with your ship kit to access the HP licensing web site through your internet browser, enter the serial number and registration number, and obtain a license key.

Feature Keys

Feature keys verify ownership of the Element Manager and optional features that can be purchased for the Element Manager. The feature key, which is encoded with a switch or director's serial number, can only be configured on the switch or director to which it is assigned.

When you purchase additional Element Manager features, you receive a feature key. The feature keys that you are currently using are included in this key.

Here are some important notes about the Element Manager feature key introduced with this release:

- All edge switches and directors that were purchased prior to the release of firmware 06.00.00 will automatically have the Element Manager feature enabled when their firmware is upgraded to version 06.00.00 or later. However, the feature key for the Element Manager will not be added or incorporated into the existing feature key.

- Enabling the **Reset Configuration** option through the Element Manager **Maintenance** menu clears all features that were enabled through the Configure Feature Key dialog box. When you attempt to reinstall features using a feature key assigned for an edge switch or director prior to the release of 06.00.00, a warning displays that the Element Manager feature key is not installed. You must contact customer support to get a feature key reassigned that includes the Element Manager feature.
- For directors and switches shipped with firmware 6.0 or later installed:
  - Directors - The Element Manager enablement certificate is included with the unit as shipped.
  - Switches - The Element Manager is optional. When you want to manage a switch through an Element Manager, you will receive an enablement certificate with which you can obtain a Feature Key. You must activate this key through the configure Feature Key dialog box.

Introduction to High Availability Fabric Management

The High Availability Fabric Manager (HAFM) is a Java-based graphical user interface (GUI) that enables you to manage users and products, monitor products, and open Element Managers.

HAFM Release 8.x is available for installation on the 1U rack-mount appliance (HAFM appliance). HAFM 8.x has the ability to manage large fabrics and provides more functionality.

The HAFM application is installed on the HAFM appliance to provide local access to managed products. *HAFM Client* applications can also be installed on remote user workstations to provide remote access to the managed products through the HAFM appliance. A maximum of nine concurrent users (eight remote and one local HAFM appliance user) can log in to the *HAFM* application.

When using two LAN connections (public and private) at the HAFM server, Microsoft Windows and the HAFM application determine the following:

- Which LAN is to be the private LAN for communication between the HAFM server, and the directors and edge switches that the HAFM server manages.
- Which LAN is to be the public LAN for communication between the HAFM server and computers seeking remote client access to the HAFM server.

Either LAN connection on the HAFM server can be the public LAN or the private LAN. Though the directors and edge switches can be managed via either LAN, the public LAN is the only one that can support remote client access. Thus, if one attempts to access the HAFM server via a remote client session and is unknowingly using what has been designated as the private LAN, the remote session will not be allowed. The IP address that the HAFM server has determined to be the public LAN which supports remote client access, displays in the title bar of the main window of the HAFM application which displays after logging in to the HAFM application.

The HAFM application designates the public LAN as the first LAN detected whose IP address is not the reserved private subnet 10.x.x.x. Thus, if neither IP address is 10.x.x.x, the first LAN detected by HAFM is designated as the public LAN. This order of detection is influenced by Microsoft Windows and not guaranteed.

For a dual LAN configuration, both LANs must be connected when the HAFM server is booted up. If only one is connected, the HAFM server interprets this as a single LAN configuration, and the connected LAN will be designated as the LAN for remote client sessions.

There are a two ways to assure the pubic and private designations of the LANs.

- If you use a private LAN IP address, i.e. 10.x.x.x, this causes this LAN to be designated as the private LAN. You must also have the public LAN connection active when the HAFM server is booting up, or else the *HAFM* application will interpret this as a single LAN connection configuration, and the 10.x.x.x LAN will be designated as the LAN for remote client sessions.
- You can configure a specified Ethernet interface on the HAFM server to be the public LAN (to listen for remote client connections). To configure this feature, you must manually edit a file on the HAFM server to explicitly specify which IP address HAFM should use as the public LAN.
- Perform the following to configure an Ethernet interface:
  - Open the `config.properties` file in directory `C:\Program Files\HAFM\`, and add the following line:

    `ServerRmiIpAddress=x.x.x.x`

    where `x.x.x.x` is the IP address assigned to one of the Ethernet LAN adapters which is to be used as the public LAN. This entry is case sensitive and must be made exactly as shown. Once this line has been added, the HAFM server must be rebooted.

Note: This does not impact the Fibre Channel operations of any edge switch or director. Only monitoring switch operations, logging events, and implementing configuration changes are interrupted.

If the public LAN IP address of the HAFM server is ever changed, this file must be edited again to reflect the new IP address.

Remote workstations are not supported on the secondary adapter, and must always connect to the public adapter as shown in Figure 2.

For details on configuring remote workstations, see "Configuring Remote Workstations" on page 251.

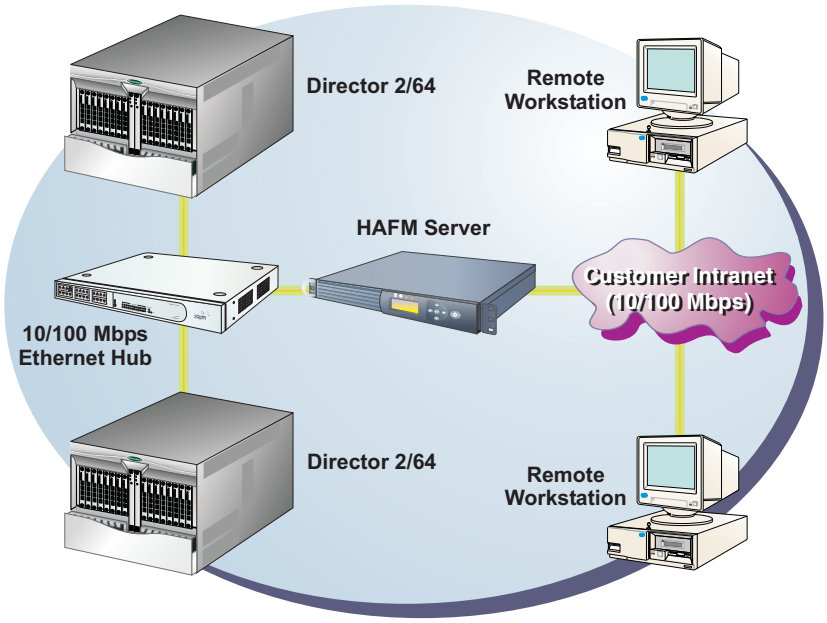


Figure 2: Product management options

Besides the HAFM and Element Managers on the HAFM appliance, out-of-band (non-Fibre Channel) management access to HP directors and switches is provided through the following:

- Management using simple network management protocol (SNMP). An SNMP agent is implemented through the *HAFM* application, which allows administrators on SNMP management workstations to access product management information using any standard network management tool. Administrators can assign Internet Protocol (IP) addresses and corresponding community names for up to twelve SNMP workstations functioning as SNMP trap message recipients.
- Management through the Internet using the Embedded Web Server (EWS) interface installed on the director or switch. This interface supports configuration, statistics monitoring, and basic operation of the product, but does not offer all the capabilities of the corresponding Element Manager in HAFM. Administrators launch the web server interface from a remote PC by entering the product's IP address as the Internet uniform resource locator (URL), then entering a user name and password at a login screen. The PC browser then becomes a management console.

- Management through a PC-based Telnet session using the command line interface (CLI). Any platform that supports Telnet client software can be used.

HAFM Appliance Information

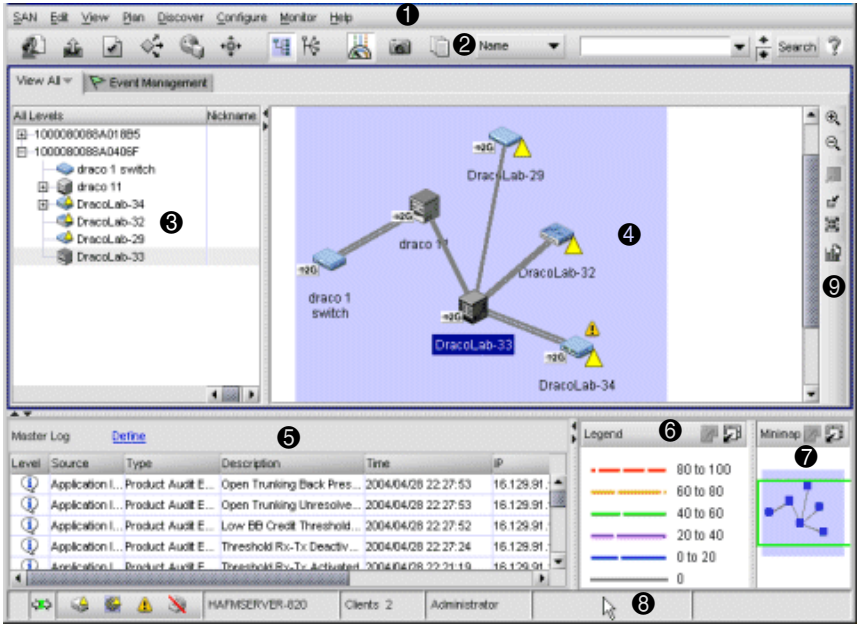
The HAFM appliance provides a central point of control for managed Fibre Channel products. The HAFM appliance is required for installing, configuring, and managing these products.

Note: Although products can perform normal operations without an HAFM appliance, the HAFM appliance should operate at all times to monitor product operations, report failures, log event changes, and log configuration changes.

User Interface Description

The main window is comprised of various areas. Descriptions are listed below the graphic.

Note: Some panels may be hidden by default. To view all panels, choose **View > All Panels**, or press **F12**.



❶ Menu Bar
❷ Toolbar
❸ Product List
❹ Physical/Topology Map
❺ Master Log
❻ Connection Utilization Legend
❼ Minimap
❽ Status Bar
❾ Toolbox

Figure 3: View All - HAFM 8 window

Menu Bar

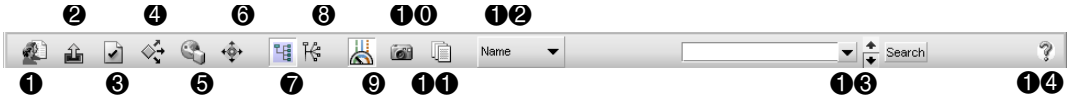
The menu bar as shown in Figure 4, is located across the top of the main window. Pull-down menus are displayed by clicking on the menu bar option with the mouse, or by pressing **ALT** with the underlined letter of the name for the menu bar option.

❶ SAN menu
❷ Edit menu
❸ View menu
❹ Plan menu
❺ Discover menu
❻ Configure menu
❼ Monitor menu
❽ Help

Figure 4: Menu bar

Toolbar

The toolbar as shown in Figure 5, is located at the top of the main window below the Menu bar. The Toolbar provides buttons to perform various functions.



❶ HAFM 8 Users
❷ Export
❸ Properties
❹ Launch Element Manager
❺ Discover Setup
❻ Zoning
❼ Discovered SAN
❽ Planned SAN
❾ View Utilization
❿ Persist Fabric
⓫ View Report
⓬ Label With
⓭ Search
⓮ Help

Figure 5: Toolbar

Note: Depending on your licensed modules, the buttons on your toolbar may differ.

Product List

The Product List, located on the **View** tab, displays an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses. To display the Product List, choose **View > Product List**, or press **F9**.

You can edit information in the Product List by double-clicking in a field marked with a green triangle. You can sort the Product List by clicking a column heading.

Physical/Topology Map

The Physical/Topology Map is the map of the topology that displays when you select the **View** tab on the main window. The Physical Map displays devices and their connections and ports. A topology is a logical and/or physical arrangement of devices on a network.

Master Log

The Master Log as shown in Figure 6, is located in the lower left area of the main window. The Master Log lists the events that occurred on the SAN. If you do not see the Master Log, choose **View > All Panels**. The default locations for the log files are listed below:

- `<Install_Home>\Server\Universe_Home\Test Universe\_Working\EventStorageProvider\event.log`
- `<Install_Home>\Server\Local_Root\EventStorage Provider\event.log`

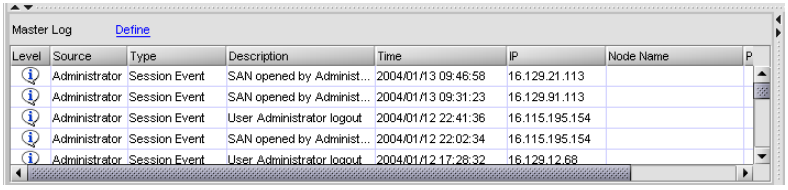


Figure 6: Master Log

The following fields and columns are included in the Master Log.

- **Level**—The severity of the event.

Table 2: Event Icons

Event Icon	Description
	Informational
	Warning
	Fatal

- **Source**—The product on which the event occurred.
- **Type**—The type of event that was performed (for example, client/server communication events).
- **Description**—Description of the event.
- **Time**—The time and date the event occurred.
- **IP**—The IP address of the product on which the event occurred.
- **Node Name**—The name of the node on which the event occurred.
- **Port Name**—The name of the port on which the event occurred.

Connection Utilization Legend

The Connection Utilization Legend as shown in Figure 7, is located in the lower right-hand area of the main window. The Legend displays the percentage of utilization on the trunks as well as on the utilization legend (below). To display the connection utilization, choose **Monitor > Utilization > On**, or **CTRL+U**.

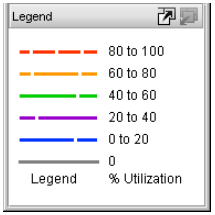


Figure 7: Connection Utilization Legend

In Table 3, the color and the length of the lines indicate the bandwidth utilization.

Table 3: Connection Utilization Legend

Line Color	Utilization
Red line	80% to 100% utilization
Orange line	60% to 80% utilization
Light green line	40% to 60% utilization
Dark purple line	20% to 40% utilization
Blue line	0% to 20% utilization
Gray line	0% utilization

To turn utilization off, choose **Monitor > Utilization > Off**.

Minimap

The Minimap as shown in Figure 8, is located in the lower right-hand corner of the main window. The Minimap is useful for getting a bird's-eye view of the SAN, or to quickly jump to a specific place on the Physical Map. To jump to a specific location on the Physical Map, click that area on the Minimap. A close-up view of the selected location is displayed on the Physical Map.

Use the Minimap to view the entire SAN and to navigate more detailed map views. This feature is especially useful if you have a large SAN.

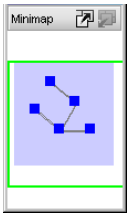


Figure 8: Minimap

Floating the Minimap

To float the Minimap and view it in a separate window, click the **Detach** button () in the upper right-hand corner of the Minimap.

Anchoring the Minimap

To return the Minimap to its original location on the main window, do one of the following:

- Click the **Attach** button () in the upper right-hand corner of the Minimap.
- Click the **Close** button () in the upper right-hand corner of the Minimap.
- Click the logo in the upper left-hand corner of the Minimap and choose **Close**, or **ALT+F4**.

Resizing the Minimap

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow displays. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow displays. Click and drag to change the window size.

Status Bar

The status bar as shown in Figure 9, is located at the bottom of the main window. The status bar provides a variety of information about the SAN and the application. The icons on the status bar may change to reflect different information.

Note: Depending on your configuration, some status bar icons may not display.

❶ Server Status
❷ Connection Status
❸ Product Status
❹ Fabric Status
❺ Attention Indicator
❻ Call-Home Status
❼ Server Name
❽ Client Count
❾ User's Access Level

Figure 9: Status Bar

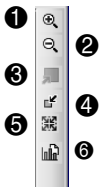
- **Server Status**—Displays local Server status.
- **Connection Status**—Displays the appliance-client connection status.
- **Product Status**—Displays the most degraded status of all devices in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status displays as degraded. Click this icon to open the Product State Log. See "Determining a Product's Operational Status" on page 98 for more information.
- **Fabric Status**—Displays the state of the fabric that is least operational, based on ISL status.
- **Attention Indicator**—Displays when at least one HP product in the SAN has an attention indicator. Click the icon to open the Service Request dialog box, which lists all HP switches and directors that need attention.
- **Call-Home Status**—Displays if the Call-Home service has been enabled. If Call-Home has been enabled on all managed HP switches and on the *HAFM* application, the icon displays as enabled. If Call-Home is disabled on any one of the HP switches or on the *HAFM* application, the icon displays as disabled.

Click the icon to open the Call Home Settings Summary dialog box, which lists whether the Call-Home feature is enabled on the *HAFM* application and on each managed HP switch or director.

- **Server Name**—Displays the name of the Server to which you are connected.
- **Client Count**—Displays the number of clients.
- **User's Access Level**—Displays the user ID of the logged in user.

Toolbox

The toolbox as shown in Figure 10, is located at the top right-hand side of the Physical/Topology Map window. The Toolbox provides tools to zoom in and out of the Physical Map, collapse and expand groups, and fit the topology to the window, and generate Physical Map reports.



❶ Zoom In
❷ Zoom Out
❸ Expand
❹ Collapse
❺ Fit In View
❻ Generate Physical Map Report

Figure 10: The Toolbox

Searching the Online Help

To find all the help topics that contain a particular word or phrase:

1. On the Help window, click the tab with the magnifying glass icon.
2. In the **Find** field, enter the word or phrase for which you want to search.
3. Press **Enter**.

If any matches are found, a list of topics displays in the panel. The number of times the word or phrase occurs in the topic displays next to the name. Click the name to display that topic.

Backing Up and Restoring Data

For instructions on backing up and restoring data to the 1U HAFM appliance, see "HAFM Appliance Backup and Restore" on page 93.

Setting Up the Application

This chapter provides instructions for setting up and customizing the application.

Configuring an Appliance

If you are using a new HAFM appliance with HAFM 08.02.00 installed, follow the instructions in the *HA-Fabric Manager Appliance Installation Guide* to install your HAFM appliance. If you are upgrading the HAFM application on an existing HAFM appliance, follow the instructions in "Upgrading the HAFM Application" on page 47.

The application is comprised of two parts: the server (which runs only on the HAFM appliance) and the client. The server is installed on one HAFM appliance and stores SAN-related information; it does not have a user interface. To view SAN information through a user interface, you must log in to the server running on the appliance through a client.

Note: The server and client(s) may reside on the same machine, or on separate machines.

In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between the server application running on HAFM appliances and clients. In other words, a client can find a server, appear to log in, but immediately is logged out because the server cannot reach the client. To resolve this issue, the application automatically detects the network configuration and runs the client in "polling mode" when necessary.

When the client is not running in polling mode, the server calls the client whenever it has new data. When the client is running in polling mode, the server queues up the data and the client periodically checks in (approximately every 5 or 10 seconds) and gets the data.

Configuring a New HAFM Appliance

In order to activate the application, you need to request a license key. Once you have activated the application, go to "Accessing HAFM" on page 47 for further instructions.

Getting a License Key for New Software

If you just purchased the application, use these instructions to obtain your license key:

1. Go to the URL listed on the software entitlement request certificate for HAFM and click **generate a license key**.

2. Enter the Registration Number in the **Registration Number** field.
3. Click **next**.
4. Enter the serial number in the **Serial Number** field. You can find the serial number on the back of the software CD case. You can also enter the registration numbers for other HAFM application features you have purchased, or you can enable these at a later time if you wish.
5. Enter the required registration information.
6. Click **next**.
7. Confirm the existing and new features to be enabled.
8. Click **next**.
9. The license key and all enabled features display. Print or send an e-mail containing the information to retain a copy for your records. You need to enter this key during the installation process. See "Upgrading the HAFM Application" on page 47 for further instructions.

Retrieving Lost Keys

If you have lost your license key:

1. Go to the URL listed on the software entitlement request certificate for HAFM.
2. Click **reprint license certificates**.
3. Enter your product's serial number or key, and select **switches** from the **Hardware Platform** drop-down menu
4. Click **next**. The license key and the enabled feature information displays. Print or e-mail the information to retain a copy for your records.

Entering a License Key

A license key is required to run the application. The key specifies the maximum number of switch ports you can monitor, the number of clients you can run, the expiration date of a temporary license, as well as any licensed optional features or modules.

1. Choose **Help > License**. The License dialog box displays, as shown in Figure 11.

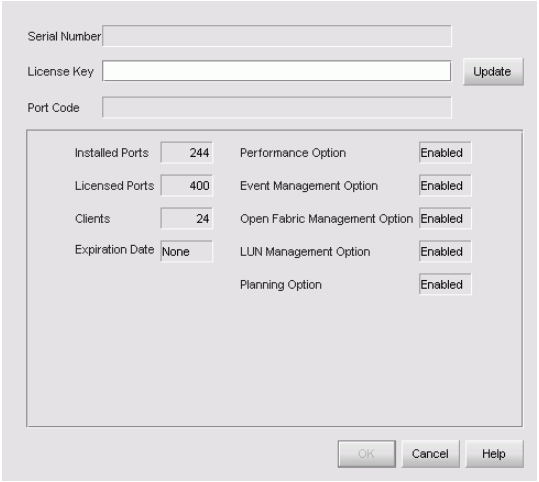


Figure 11: License dialog box

2. Enter the license key in the **License Key** field.

Note: The **License Key** field is not case-sensitive.

---

3. Click **Update** and ensure that the information is accurate.

Note: The License dialog box displays the license information for the appliance to which the client is currently connected. When you click **Update**, the dialog box decodes the key you entered and displays the new license information without setting a new license on the appliance. The information is set on the appliance only when you click **OK**.

---

4. Click **OK** to enable the software. The application automatically logs out and the Log In dialog box displays. Log in using the instructions in "Accessing HAFM" on page 47.

Entering a Feature License Key

1. Choose **Help > License**. The License dialog box displays, as shown in Figure 11.
2. Enter the new license key into the **License Key** field.

Note: The **License Key** field is not case-sensitive.

3. Click **Update** and ensure that the information is accurate.
4. Click **OK** to enable the software. The application automatically logs out and the Log In dialog box displays. Log in using the instructions in "Accessing HAFM" on page 47.

Ordering Additional Features

To order new features or increase managed port capabilities, contact your sales representative.

Upgrading the HAFM Application

For instructions on upgrading the HAFM application, refer to the *HP StorageWorks HAFM 7.x to 8.0 Transition Guide.*

Uninstalling the Appliance

Follow these instructions to uninstall the application from your system.

1. Choose **Start > Programs > HP StorageWorks ha-fabric manager > Uninstall**.
2. The InstallShield wizard takes you through the uninstallation process.

Uninstalling the HAFM Client

Follow these instructions to uninstall the application from your system.

1. Choose **Start > Programs > HP HAFM > Uninstall**.
2. The InstallShield wizard takes you through the uninstallation process.

Accessing HAFM

You can access HAFM using one of the following methods:

Accessing HAFM on the HAFM Appliance

You can log in to HAFM located on the appliance from a browser-capable PC connected through an Ethernet LAN segment. Use the following steps:

1. Ensure the HAFM appliance and a browser-capable PC are connected through an Ethernet LAN segment. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
2. At the PC browser, enter the URL in the following format:

   `http://xxx.xxx.xxx.xxx:5800`

   Where `xxx.xxx.xxx.xxx` is the default IP address or the IP address configured for the appliance during installation. The VNC Authentication window displays, as shown in Figure 12.

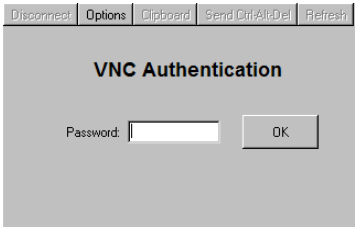


Figure 12: VNC Authentication window

3. Type the password and click **OK**. The **Welcome to Windows** dialog box displays, as shown in Figure 13.

Note: The default TightVNC viewer password is **password.**

Figure 13: Welcome to Windows dialog box

4. Click **Send Ctrl-Alt-Del** at the top of the window to log on to the HAFM appliance desktop. The **Log On to Windows** dialog box displays, as shown in Figure 14.

Note: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the HAFM appliance.

Figure 14: Log On to Windows dialog box

5. Type the Windows 2000 user name and password and click **OK**. The HAFM 8 Log In dialog box displays, as shown in Figure 15.

Note: The default Windows 2000 user name is **Administrator** and the default password is **password**. The user name and password are case-sensitive.

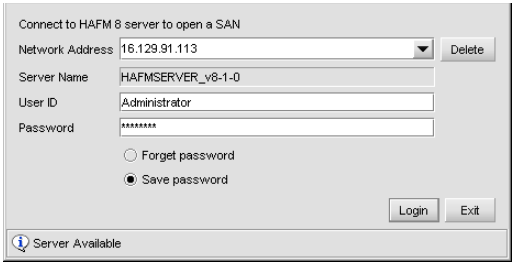


Figure 15: HAFM Log In dialog box

6. Enter the HAFM appliance IP address in the **Network Address** field.

The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged in to.

If you are logging in to the local HAFM appliance, the network address is *localhost*.

If you want to connect to an HAFM appliance that is not listed, enter the IP address in the **Network Address** field.

7. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.

Note: If user names have not been established, you can use the default user name Administrator and password password. The user name and password are case-sensitive. HP recommends that you change the default password as soon as possible.

To add or modify user names, passwords, and user rights, see the appropriate subsections in "Managing Users" on page 57.

8. If you want your computer to save the login information, choose the **Save Password** option.
9. Click **Login**. The View All - HAFM 8 window displays, as shown in Figure 16.

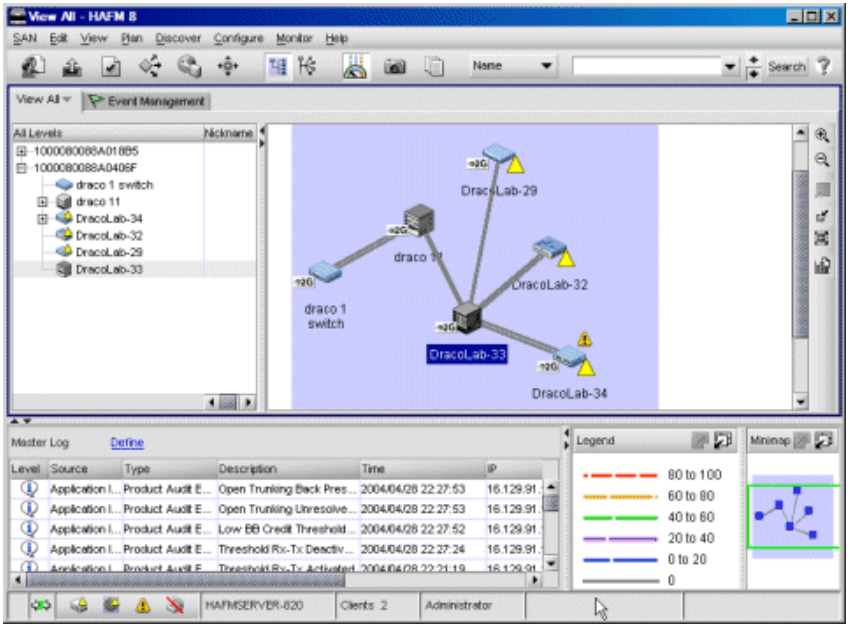


Figure 16: View All - HAFM window

Accessing Remote HAFM appliances

You can use the *HAFM Client* applications to remotely access an HAFM appliance. You must have the *HAFM Client* application installed on your computer before proceeding. See instructions for *HAFM Client* application installation in "Configuring Remote Workstations" on page 251.

To access remote HAFM appliances, perform the following:

1. Start the HAFM Client application by following the instructions in "Starting HAFM on Remote Workstations" on page 55.
2. Enter the appliance's network address in the HAFM 8 Log In dialog box, as shown in Figure 15.
3. Enter the HAFM appliance IP address in the **Network Address** field.

   The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged in to.

If you want to connect to an HAFM appliance that is not listed, enter the IP address in the **Network Address** field.

4. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.

Note: If user names have not been established, you can use the default user name (Administrator) and password (password). The user name and password are case-sensitive. HP recommends that you change the default password as soon as possible.

To add or modify user names, passwords, and user rights, see the appropriate subsections in "Managing Users" on page 57.

5. If you want your computer to save the login information, choose the **Save Password** option.
6. Click **Login**. The View All - HAFM 8 window displays, as shown in Figure 16.

If the HAFM window displays, you have logged in to the appliance. The network address you entered remains in the **Network Address** drop-down list for future logins. If you fail to connect to the appliance, the network address does not remain in the list.

Adding an Appliance to the Log In Dialog Box List of Appliances

1. Start the HAFM application on the HAFM appliance, as described in "Accessing HAFM on the HAFM Appliance" on page 48, or on a remote workstation, as described in "Starting HAFM on Remote Workstations" on page 55. The HAFM 8 Log In dialog box displays, as shown in Figure 15.
2. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the Network Address is `localhost`.

   The default address that displays in the **Network Address** field is the address of the last appliance accessed. Click the **Network Address** drop down list to see the network addresses of all HAFM appliances that were accessed from the computer you are logged in to.

   If you want to connect to an HAFM appliance that is not listed, enter the IP address in the **Network Address** field.

3. Enter your user name and password in the **User ID** and **Password** fields. User names and passwords are case-sensitive.

Note: You must have an established login and password account on the new HAFM appliance.

4. If you want your computer to save the login information, choose the **Save Password** option.
5. Click **Login**. The View All - HAFM 8 window displays, as shown in Figure 16.

Removing an Appliance from the Log In Dialog Box List of Appliances

You can remove appliances from the list in the HAFM 8 Log In dialog box.

1. Turn on the HAFM appliance, or if the appliance is already turned on, double-click the **HAFM** icon on the desktop. The HAFM 8 Log In dialog box displays, as shown in Figure 15.
2. Select the appliance you want to remove from the **Network Address** drop-down list. The selected appliance's IP address displays in the **Network Address** field.
3. Click **Delete**.

Note: The Appliance is deleted from your **Network Address** drop-down list without confirmation.

Logging Out of an Appliance

To log in to a different appliance, you must first log out of the current appliance.

1. Choose **SAN > Log Out**. You are logged out of the current appliance and the HAFM 8 Log In dialog box displays, as shown in Figure 15.
2. See "Accessing HAFM" on page 47 for instructions on logging in to a new appliance.

Starting and Stopping HAFM Services

Options are available for starting and stopping HAFM Services through the desktop Start menu:

1. Choose **Start > Programs > HP StorageWorks ha-fabric manager**.
2. Choose **Stop Services** to stop all HAFM services and HAFM appliance functions.
3. Choose **Start Services** to restart these functions.

HAFM Services is the software application that provides services to the *HAFM* application. HAFM Services runs only on the HAFM appliance.

Managing Remote Access to the HAFM Appliance

Users at the HAFM appliance can access the HAFM and Element Managers loaded on the appliance itself. Users at remote PC workstations can also access the same HAFM appliance or other HAFM appliances if the workstations meet minimum hardware and software requirements and are running the *HAFM Client* application. Workstations must also be configured to connect with the HAFM appliance over a TCP/IP network connection.

Figure 2 on page 33 illustrates a remote user workstation connected to the HAFM appliance through a LAN. Please note that this is an example configuration only.

Operators at remote workstations can manage and monitor all products controlled by the HAFM appliance. Each active connection between a remote workstation and an HAFM appliance and managed products is called a session. A maximum of nine concurrent users (eight remote and one local HAFM appliance user) can log in to the *HAFM* application.

Requirements for Remote Workstations

The HAFM is downloaded and installed on user workstations from the HAFM appliance. The remote workstations can be Windows 2000, Windows NT, Windows XP, HP-UX, AIX, Linux, or Solaris systems.

For the minimum system requirements for remote workstations, see Appendix D in this guide for the appropriate operating system.

Installing Software on Remote Workstations

For procedures to install HAFM software on remote user workstations and configure the workstations for connection to an HAFM appliance, see Appendix D in this guide for the appropriate operating system.

Starting HAFM on Remote Workstations

If the *HAFM* application is not running or the HAFM 8 Log In dialog box is not displayed on your remote workstation, you can start the application by following the appropriate steps for your workstation's operating system.

Starting HAFM on a Windows System

To start the *HAFM* application on a Windows 2000, Windows NT, or Windows XP system:

1. Start the *HAFM Client* application using one of the following options:
   - Choose **Start > Programs > HP HAFM > HAFM 8.x**.
   - Double-click the **HAFM 8.x** desktop icon.
2. Enter the Network Address, User ID, and Password for the HAFM appliance you intend to access.

Note: The default User ID is **Administrator**, and the default password is **password**.

---

3. Click the **Login** button. The HAFM client accesses the HAFM appliance, and the **View All - HAFM 8** window displays, as shown in Figure 16.

Starting HAFM on an HP-UX, AIX, Linux, or Solaris System

To start the *HAFM* application on an HP-UX, AIX, Linux, or Solaris system from the home directory:

Note: If you have saved the *HAFM* application in a different location, type in the appropriate directory names.

---

1. Go to the location where you installed the application (the default is `/usr`).

2. Start the appliance and client:

   ```
   ./HAFM
   ```

3. If you want to start the client only:

   ```
   ./Client
   ```

   or

   Go to the `bin` directory in the location where you installed the application (the default is `/opt/`).

   ```
   cd /<path>/HAFM 8.0/bin
   ```

4. Start the appliance.

   ```
   ./HAFM_Mgr start
   ```

5. Start the client.

   ```
   ./HAFM_Client
   ```

Managing Users

To grant access to the HAFM application, the administrator can assign user names, passwords, and access rights to users. The administrator can configure up to sixteen users in the HAFM application, but no more than nine users (eight remote and one local user) can simultaneously access one HAFM appliance.

Viewing the List of Users

Perform the following to view a list of users, their event notification settings, and their e-mail addresses:

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17.

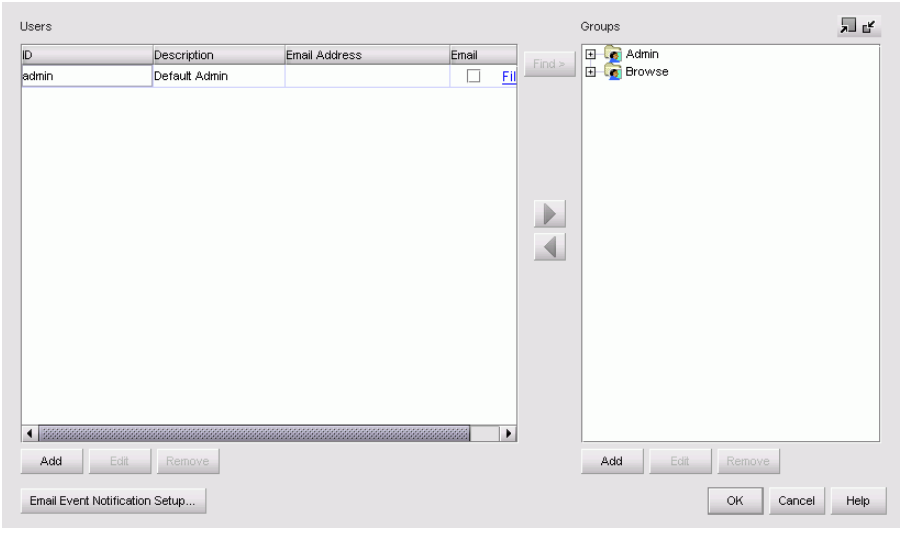


Figure 17: HAFM 8 Server Users dialog box

Adding a User Account

Note: You must be an administrator to perform this task.

Perform the following to add a user:

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17.
2. Click **Add**. The Add User dialog box displays, as shown Figure 18.

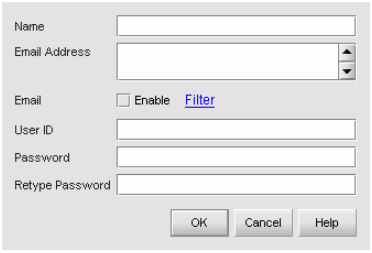


Figure 18: Add User dialog box

3. Enter the name in the **Name** field.
4. Enter the users' email addresses in the **Email Address** field, separating multiple addresses with a semicolon.
5. Click the **Enable** check box to enable e-mail notification for the user.

   A message may display stating that you must enable event notification for the SAN. Click **Yes**.
6. Click the **Filter** link to specify the event types for which to send e-mail notification to this user. See "Filtering Event Notifications for a User" on page 60 for detailed instructions.
7. Enter the user name in the **User ID** field.
8. Enter the user's password in the **Password** field.
9. Enter the password again in the **Retype Password** field.
10. Click **OK**. The new user displays on the HAFM 8 Server Users dialog box.
11. Click **OK** to close the HAFM 8 Server Users dialog box.

Changing a User Account

Note: You must be an administrator to perform this task.

Perform the following to modify an existing user:

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17.
2. Highlight the user whose information you want to edit from the Users table.
3. Click **Edit**. The **Change User** dialog box displays, as shown in Figure 19.

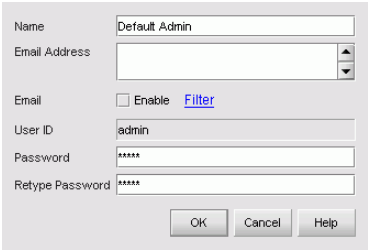


Figure 19: Change User dialog box

4. Edit the information as necessary.
5. Click **OK**. The edited information displays on the HAFM 8 Server Users dialog box.
6. Click **OK** to close the HAFM 8 Server Users dialog box.

Removing a User Account

Note: You must be an administrator to perform this task.

Note: You are not prompted for confirmation before the user's account is removed. If the user is logged in when you remove their account, they are not affected until they log out and try to log in again.

Perform the following to remove a user:

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17.
2. Highlight the user account you want to remove.
3. Click **Remove**.

4. Click **OK**.

Filtering Event Notifications for a User

Note: You must be an administrator to perform this task.

The application provides notification of many different types of SAN events. If a user only wants to receive notification of certain events, you can filter the events specifically for that user.

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17.
2. Click the **Filter** link in the **Email** column associated with the user for whom you want to filter events. The Define Filter dialog box displays, as shown in Figure 20.

   The **Selected Events** table includes the events of which this user is notified. The **Available Events** table includes all other events.

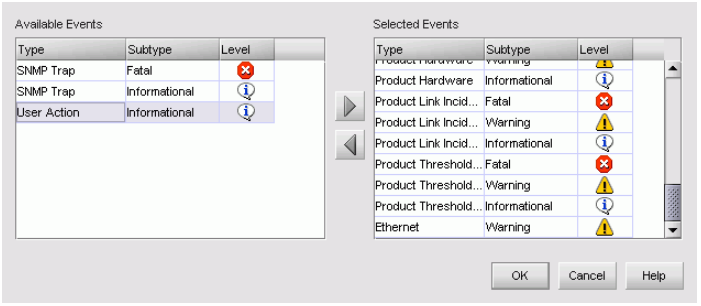


Figure 20: Define Filter dialog box

3. Move events between the tables by selecting the event and clicking the appropriate arrow button.
4. Click **OK**. The HAFM 8 Server Users dialog box displays.
5. Turn on event notification for the user by choosing the **Filter** check box.
6. Click **OK**.

Configuring Remote Access

You can specify the network addresses that can have access to the appliance. Perform the following to configure remote access:

1. Choose **SAN > Remote Access**. The Remote Access dialog box displays, as shown in Figure 21.

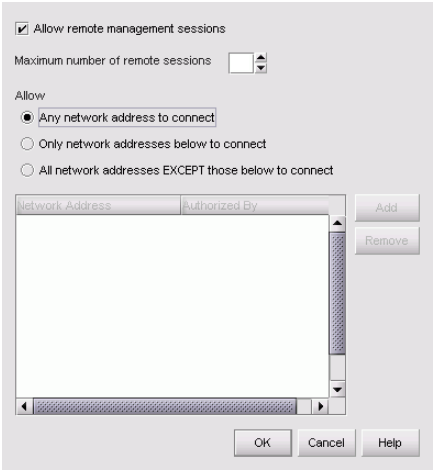


Figure 21: Remote Access dialog box

2. Choose the **Allow remote management sessions** check box to allow others to access the appliance remotely.
3. Enter the maximum number of remote sessions you want to allow.
4. Choose whether to allow all or some network addresses to connect from the **Allow** options.
5. If you selected **Only network addresses below to connect** or **All network addresses EXCEPT those below to connect**, add and remove addresses in the table at the bottom of the dialog box.
   - To add an address, click **Add**, enter a network address, and click **OK**.
   - To remove an address, select the address from the table and click **Remove**.
6. Click **OK**.

Viewing Active User Sessions

A maximum of nine concurrent users (eight remote and one local HAFM appliance user) can log in to the *HAFM* application. Since more than one client can access an appliance at a time, monitoring clients can be an important part of maintaining the SAN. View active user sessions to determine which clients are logged in to the appliance.

To display the Active Sessions dialog box:

1. Choose **SAN > Active Sessions**. The Active Sessions dialog box displays, as shown in Figure 22.

   The Active Sessions dialog box lists the connected users, their network addresses, and the date and time of when they logged in. If a user is logged in from more than one location, there is a separate entry for each session.

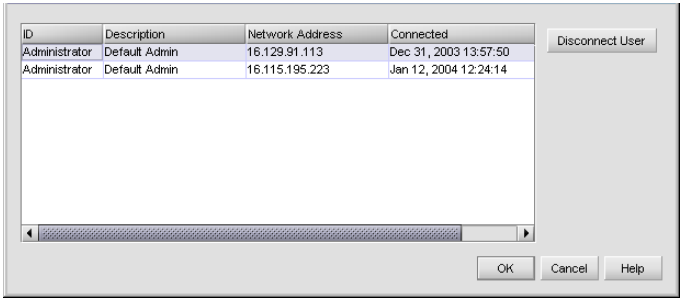


Figure 22: Active Sessions dialog box

The Active Sessions dialog box displays active session information in this format:

- **ID**—The id of the current user.
- **Description**—The description of the user.
- **Network Address**—The network address of the current user.
- **Connected**—The date and time that the session was established.

Disconnecting a User

If you have administrator privileges, you can disconnect users. To disconnect a user, perform the following:

1. Highlight the user that you want to disconnect and click **Disconnect User**. A message box displays, as shown in Figure 23.

Figure 23: Disconnect User message box

2. Click **Yes**.

   The user is disconnected. The appliance immediately shuts down the appliance-client connection. The status bar on the client displays that the appliance connection was lost. All products and connections on the Physical Map stay in the condition they were in when the session ended; they do not turn grey. The client displays a message stating that a user disconnected the client from the appliance.

Note: To prevent this user from reconnecting, remove the user account through the HAFM 8 Server Users dialog box. See "Removing a User Account" on page 59 for instructions.

Managing User Groups

This section provides an overview of user groups and their access levels and describes how to set up a user group.

About User Groups and Access Levels

A user with administrative privileges ("System Administrator") can assign users to user groups. Four pre-configured user groups are available with the application; however, System Administrator users can also create user groups manually. See "Creating a User Group" on page 64 for instructions.

Table 4: User Groups and Access Levels

User Group	Description
System Administrator	Read/write access for all features: user can view and edit information; all functions are enabled and allowed.
Maintenance	Read/write access for Call Home Event Notification, Device Maintenance, and Email Event Notification Setup: user can view and edit this information. Read-only access for all other features: user can only view this information; editing and configuration capabilities are disabled.
Operator	Read/write access for Device Operation: user can view and edit this information. Read-only access for all other features: user can only view information; editing and configuration capabilities are disabled.
Product Administrator	Read/write access for Device Administration: user can view and edit this information. Read-only access for all other features: user can only view information; editing and configuration capabilities are disabled.

Creating a User Group

Note: You must be an administrator to perform this task.

You can create a user group and specify access to certain features and/or views in the application, enhancing the security of your SAN.

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17.
2. Click **Add** located below the **Groups** table. The HAFM Group dialog box displays, as shown in Figure 24.

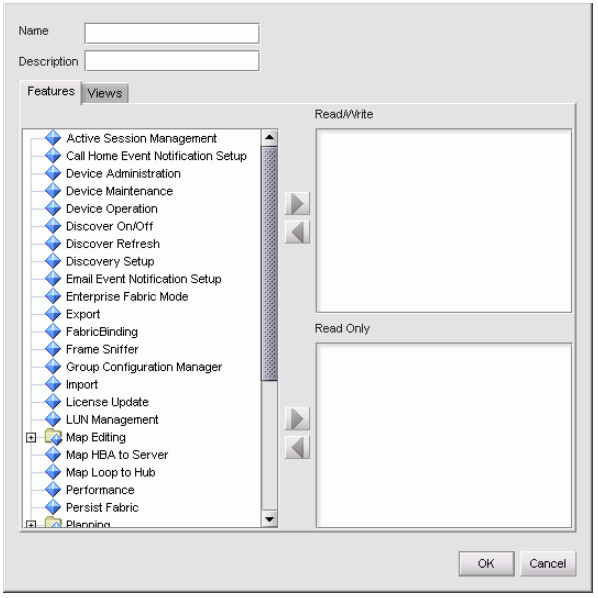


Figure 24: HAFM Group dialog box

3. Enter a name in the **Name** field.
4. Enter a description in the **Description** field.
5. If you want to assign permissions to only use certain views, click the **Views** tab and go to step 10.
   or
   If you want to assign permissions to use certain features, go to step 6.
6. Select the features for which you want to provide “read and write” access in the left-hand list. Press **CTRL** and click to select multiple features.
7. Click the right arrow next to the **Read/Write** table. The features are moved to the **Read/Write** table.

Note: If you can't assign a feature to the **Read/Write** or **Read Only** table, you don't have read access for the feature.

8. Select the features for which you want to provide "read only" access in the left-hand list. Press **CTRL** and click to select multiple features.
9. Click the right arrow next to the **Read Only** table. The features are moved to the **Read Only** table.
10. Select the views you want the user group to be permitted to access in the left-hand list. Press **CTRL** and click to make multiple selections.
11. Click the right arrow to move the selection(s) to the **Selected Views** table.
12. Click **OK**. The new group displays in the **Groups** table of the HAFM 8 Server Users dialog box. To add users to this group, follow the instructions in "Assigning Users to Groups" on page 67.
13. Click **OK**.

Changing a User Group

Note: You must be an administrator to perform this task.

You can change a user group's permissions to use certain features and views. This provides added security for your SAN as well as your management application.

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17 on page 57.
2. Click **Edit** located below the **Groups** table. The HAFM Group dialog box displays, as shown in Figure 24.
3. Change permissions as necessary. See "Creating a User Group" on page 64 for detailed instructions.
4. Click **OK**. The HAFM 8 Server Users dialog box displays.
5. Click **OK** to accept the changes made**.**

Removing User Groups

Note: You must be an administrator to perform this task.

Note: After completing these steps, the user group is removed without confirmation.

You can remove a user group regardless of whether a user is assigned to the group.

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17 on page 57.
2. Highlight the group you want to remove in the **Groups** table.
3. Click **Remove** located below the **Groups** table.
4. Click **OK**.

Assigning Users to Groups

Note: You must be an administrator to perform this task.

You can assign users to groups to assign them permissions for features and topology views. If you assign one user to multiple groups, the user has the user rights specified in all the groups.

Note: If a user is logged in when you reassign their group, they are not affected until they log out and try to log in again.

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17 on page 57.
2. Highlight a user in the **Users** table.
3. Highlight the group(s) to which you want to assign the user in the **Groups** table. Press **CTRL** and click to make multiple selections.
4. Click the right arrow button. The user is assigned to the selected groups.
5. Click **OK**.

Determining User Groups

Note: You must be an administrator to perform this task.

You can determine the groups to which a user belongs through the HAFM 8 Server Users dialog box.

1. Choose **SAN > Users**. The HAFM 8 Server Users dialog box displays, as shown in Figure 17 on page 57.
2. Highlight a user in the **Users** table.
3. Click **Find**. The groups to which the user belongs are highlighted in the **Groups** list.
4. Click **OK**.

Discovering a SAN

The application discovers products, fabrics, and connections in a SAN. Through this powerful tool, you can manage and monitor your SAN in real-time, ensuring that any issues are resolved immediately. This chapter provides instructions for configuring the discovery feature.

How Discovery Works

The application illustrates each product and its connections on the Physical Map (topology). Once you log in and configure and turn on discovery, the application discovers products connected to the SAN. See "Setting Up Discovery" on page 69 for details.

When performing out-of-band discovery, the application connects to the switches through the IP network and product information is copied from the SNS database on the switch to the appliance.

To correctly discover all SAN products, you must specify each product's IP address in the Discover Setup dialog box's **Out-of-Band** tab. If you do not configure the application to directly discover the devices, the connections and attached devices may not display correctly. Only fabrics that have HP switches as the principal switch display. If a HP switch is being directly managed, but exists in a fabric where the principal switch is a third-party device, another appliance is not allowed to connect to and manage those devices.

Setting Up Discovery

Discovery is the process by which the application contacts the devices in your SAN. In order to perform discovery, you need to specify the IP addresses for the devices in your SAN.

1. Choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 25.

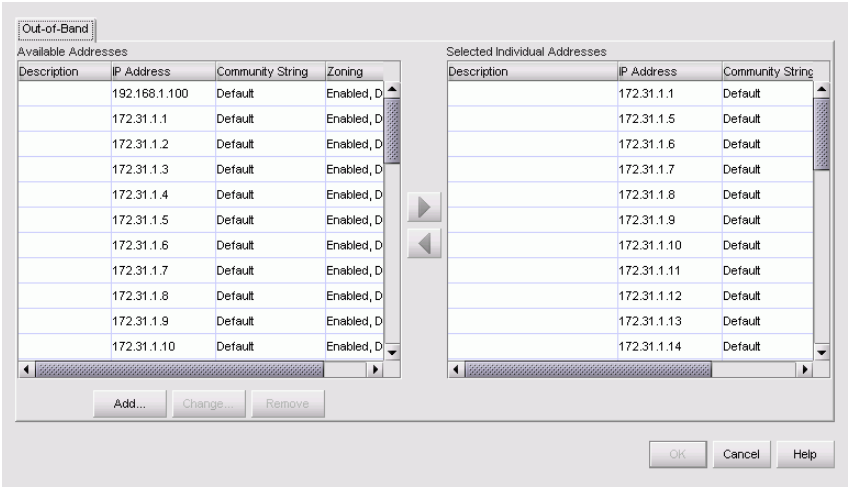


Figure 25: Discover Setup dialog box

2. Specify the IP addresses you want to discover through out-of-band discovery. You can add, change, and remove IP addresses as necessary. See "Configuring IP Addresses and Community Strings" on page 70 for instructions.

Note: To correctly discover all SAN products, you must specify each product's IP address in the Discover Setup dialog box's **Out-of-Band** tab. If you do not configure the application to discover the devices directly, the connections and attached devices may not display correctly.

---

3. Select IP addresses from the **Available Addresses** table and add them to the **Selected Individual Addresses** table by clicking the ▶ buttons.
4. Click **OK**.
5. Turn discovery on or off by choosing **Discover > On** or **Discover > Off**.

Configuring IP Addresses and Community Strings

You can configure IP addresses and community strings through which the application can perform discovery and communication functions.

Adding an IP Address

You can add IP addresses and subnets through which the SAN can be discovered. Perform the following to add an IP address:

1. Choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 25 on page 70.
2. Click **Add**. The Domain Information dialog box displays, as shown in Figure 26.

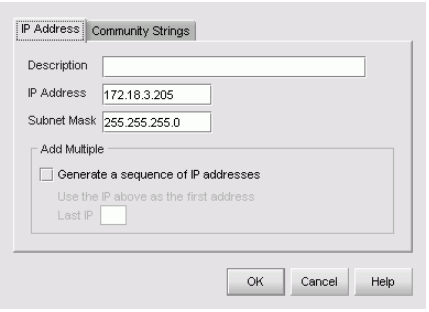


Figure 26: Domain Information dialog box (IP Address tab)

3. Enter a description for the product in **Description** field.
4. Enter the IP address in the **IP Address** field.
5. Enter the subnet mask associated with the IP address in the **Subnet Mask** field.
6. If you want to generate a sequence of IP addresses, perform the following:
   - Choose the **Generate a sequence of IP addresses** check box.
   - Enter the last IP address in the **Last IP** field.

Note: All IP addresses in a sequence must be on the same subnet and have the same first three octets.

---

7. Click **OK**.

Changing an IP Address

You can edit IP addresses or associated subnets that are listed on the Discover Setup dialog box.

1. Choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 25 on page 70.
2. Highlight the IP address in the **Available Addresses** table to edit.
3. Click **Change**. The Domain Information dialog box displays, as shown in Figure 26 on page 71.
4. Edit the information as necessary.
5. Click **OK**.
6. Click **OK** to close the Discover Setup dialog box.

Removing an IP Address

You can remove IP addresses from the Discover Setup dialog box.

1. Choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 25 on page 70.
2. Highlight the IP address in the **Available Addresses** table to remove.

Note: When you click **Remove**, the IP address is removed without confirmation.

---

3. Click **Remove**.
4. Click **OK** to close the Discover Setup dialog box.

Configuring a Community String

You can specify community strings used to communicate with products.

1. Choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 25 on page 70.
2. Click to highlight the IP address in the **Available Addresses** table to edit.
3. Click **Add**. The Domain Information dialog box displays, as shown in Figure 26 on page 71.
4. Click the **Community Strings** tab. The Community Strings tab displays, as shown in Figure 27 on page 73.

Figure 27: Domain Information dialog box (Community Strings tab)

5. Click an option in the **Read** field.
   - Choose **Default 'public'** to select the default string.
   - Choose **Custom** to specify a custom string.
6. Click an option in the **Write** field.
   - Choose **Default 'private'** to select the default string.
   - Choose **Custom** to specify a custom string.
7. If you chose **Custom** in step 5 or step 6, continue to step 8. Otherwise, skip to step 10.
8. Enter the custom string in the **Custom** field.
9. Enter the string again in the **Confirm Custom** field.
10. Click **OK**.
11. Click **OK** to close the Discover Setup dialog box.

Reverting to a Default Community String

1. Choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 25 on page 70.
2. Highlight an IP address from the **Available Addresses** table.
3. Click **Add**. The Domain Information dialog box displays, as shown in Figure 26 on page 71.
4. Click the **Community Strings** tab. The Community Strings tab displays, as shown in Figure 27 on page 73.
5. Click **Default 'public'** and **Default 'private'.**
6. Click **OK**.

Turning Discovery On and Off

Turn discovery on and off by using the Discover menu.

Turning Discovery On

Perform the following to turn discovery on:

1. Choose **Discover > On**.

Turning Discovery Off

Perform the following to turn discovery off:

1. Choose **Discovery > Off**.

Determining the Discovery State

Note: The Product List panel may be hidden by default. To view all panels, choose **View > All Panels** or press **F12**.

You can determine the discovery status of products by looking at the **Status** column in the Product List. Additionally, the operational status called “Unknown” is equivalent to the discovery state named “Offline.” The operational statuses, “Operational,” “Degraded,” and “Failed,” are equivalent to a discovery state of “Online.”

Configuring the SNMP Agent

This section provides information to help you use the SNMP Agent module.

Setting Up the SNMP Agent

The simple network management protocol (SNMP) agent module instruments the objects defined in the Fibre Channel Management (FCMGMT) Management Information Base (MIB) Version 3.1 and a small number of objects defined in MIB II. Through instrumentation of these MIB objects, the agent translates information stored on the appliance into a form usable by SNMP management stations.

You can configure network addresses and community names for up to 12 SNMP trap recipients, which receive messages through SNMP for specific events that occur on the appliance.

To configure the SNMP agent that runs on the appliance and implements the Fibre Alliance MIB, perform the following:

1. Choose **Monitor > SNMP Agent > Setup**. The SNMP Agent Setup dialog box displays, as shown in Figure 28.

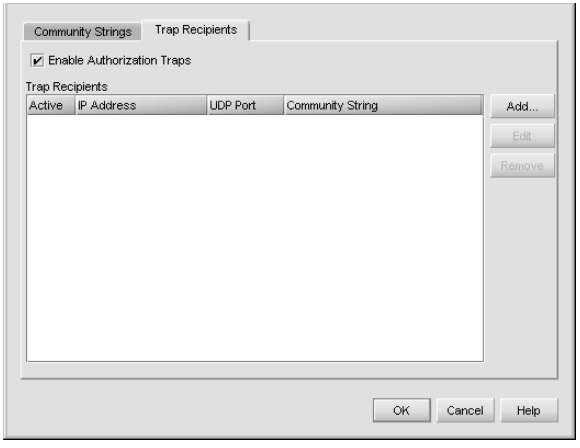


Figure 28: SNMP Agent Setup dialog box

2. Click the **Trap Recipients** tab.
3. Choose **Enable Authorization Traps** to enable or disable authorization traps to be sent when unauthorized management stations try to access SNMP information through the appliance.

4. Click **Add** to add a new trap recipient. See "Adding Trap Recipients" on page 76 for more instructions.
5. Click the recipient's row in the table and click **Edit** to edit an existing trap recipient. See "Editing Trap Recipients" on page 77 for more instructions.
6. Click **OK**.

Turning On the SNMP Agent

To turn the SNMP Agent on, perform the following:

1. Choose **Monitor > SNMP Agent > On**.

Turning Off the SNMP Agent

To turn the SNMP Agent off, perform the following:

1. Choose **Monitor > SNMP Agent > Off**.

Adding Trap Recipients

To add a trap recipient during SNMP agent configuration, perform the following:

1. Choose **Monitor > SNMP Agent > Setup**. The SNMP Agent Setup dialog box displays, as shown in Figure 28 on page 75.
2. Click the **Trap Recipients** tab.
3. Click **Add**. The Add Trap Recipient dialog box displays, as shown in Figure 29.

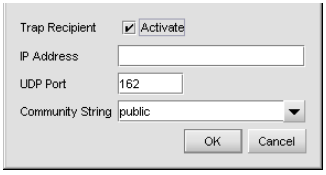


Figure 29: Add Trap Recipient dialog box

4. If you want this trap recipient to be active, ensure the **Activate** check box is selected.
5. Enter the IP address or DNS host name of the trap recipient in the **IP Address** field. This name must be 64 characters or fewer.

6. Enter the UDP port number in the **Port** field. This overrides the default User Datagram Protocol (UDP) port number for a trap recipient with any legal, decimal UDP number.
7. Choose a community string from the **Community String** drop-down list.
8. Click **OK**.

Editing Trap Recipients

To edit an existing trap recipient during SNMP agent configuration, use the following steps:

1. Choose **Monitor > SNMP Agent > Setup**. The SNMP Agent Setup dialog box displays, as shown in Figure 28 on page 75.
2. Click the **Trap Recipients** tab.
3. Click to highlight the IP address in the **Trap Recipients** table to edit.
4. Click **Edit**. The Edit Trap Recipient dialog box displays, as shown in Figure 30.

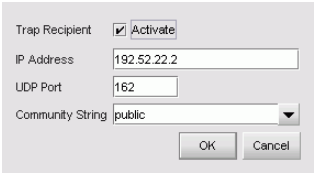


Figure 30: Edit Trap Recipient dialog box

5. Edit the fields as necessary.
6. Click **OK**.

Removing Trap Recipients

To remove an existing trap recipient during SNMP agent configuration, use the following steps:

Note: This procedure removes trap recipients without asking for confirmation.

---

1. Choose **Monitor > SNMP Agent > Setup**. The SNMP Agent Setup dialog box displays, as shown in Figure 28 on page 75.

2. Click the **Trap Recipients** tab.
3. Click the recipient's row in the table and click **Remove** to remove a trap recipient.
4. Click **OK**.

Customizing the Main Window

You can customize the main window to display only the data you need by displaying different levels of detail on the Physical Map or Product List.

You can customize the topology to display only the data you need by creating views that display certain fabrics or by displaying different levels of detail on the Physical Map. This section provides instructions for customizing the topology layout and creating user-defined views of the SAN.

If you discover or import a SAN with more than approximately 2000 devices, the devices display on the Product List, but do not display on the Physical Map. Instead, the topology area displays a message stating that the topology cannot be displayed. To resolve this issue, create a new view to filter the number of devices being discovered. See "Creating a Customized View" on page 79 for instructions.

Creating a Customized View

You may want to customize the Product List and Physical Map to simplify management of large SANs by limiting the topology size or Product List columns.

For each customized view, you can specify the fabrics that display on the Physical Map as well as the columns that display on the Product List.

Note: Customized view settings reside on the appliance; if one user creates a view, all users who log on to the same appliance are able to select that view.

---

1. Choose **View > Create View** or click the View tab and choose **Create View**. The Create View dialog box with the View Members tab displays, as shown in Figure 31.

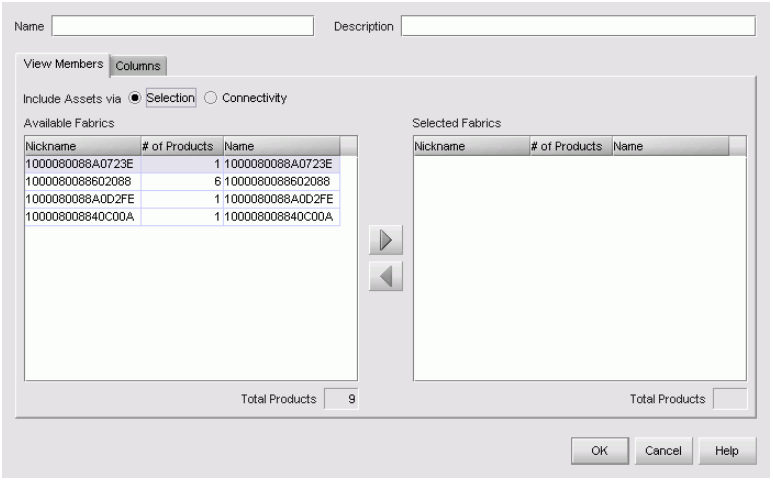


Figure 31: Create View dialog box (View Members tab)

2. Enter a name in the **Name** field.
3. Enter a description in the **Description** field.
4. If you want to filter the fabrics that display on the Physical Map, continue to step 5, otherwise go to step 8.
5. Choose **Include Assets via Selection** option.
6. Choose the fabrics you want to include in the view from the **Available Fabrics** table.

Note: "Other" in the Available Fabrics or Selected Fabrics tables refers to all isolated devices and connected sets. You see all newly discovered devices in the category even if the devices were not originally part of the view. Choose "other" to display all isolated devices.

Note: Press CTRL and click to select multiple rows.

---

7. Click the ▷ button to move your selections to the **Selected Fabrics** table.
8. If you want to show or hide Product List columns, continue to step 9, otherwise go to step 13.

9. Click the **Columns** tab. The Create View dialog box with the Columns tab displays, as shown in Figure 32.

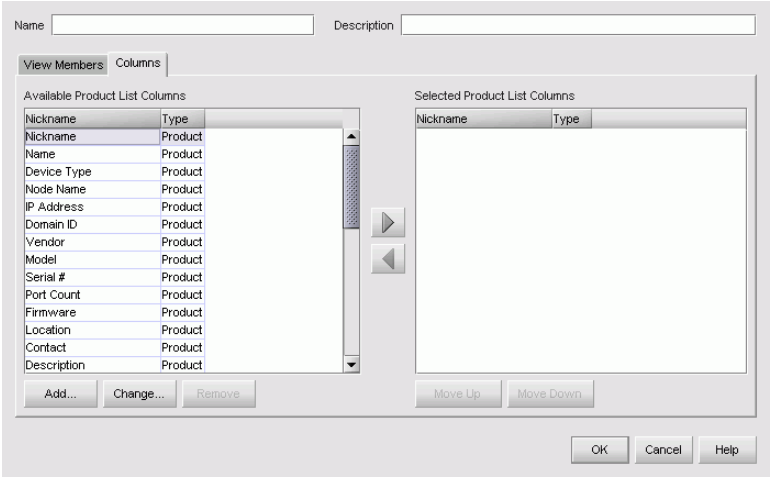


Figure 32: Create View dialog box (Columns tab)

10. Choose the columns you want to see in the Product List from the **Available Product List Columns** table.
11. Click the button to move your selections to the **Selected Product List Columns** table.
12. To add, edit, or remove columns, see "Adding a Column to the Product List" on page 84, "Changing a Column on the Product List" on page 85, and "Removing a Column from the Product List" on page 85.
13. Click **OK**. The new view automatically displays.

Note: If you select a customized view and new devices are discovered, those new devices display in the customized view.

Editing a Customized View

Note: Customized view settings reside on the appliance; if one user creates a view, all users who log on to the same appliance are able to select that view.

1. Choose the **View > Edit View**, then select the view you want to edit. The Edit View dialog box displays, as shown in Figure 33.

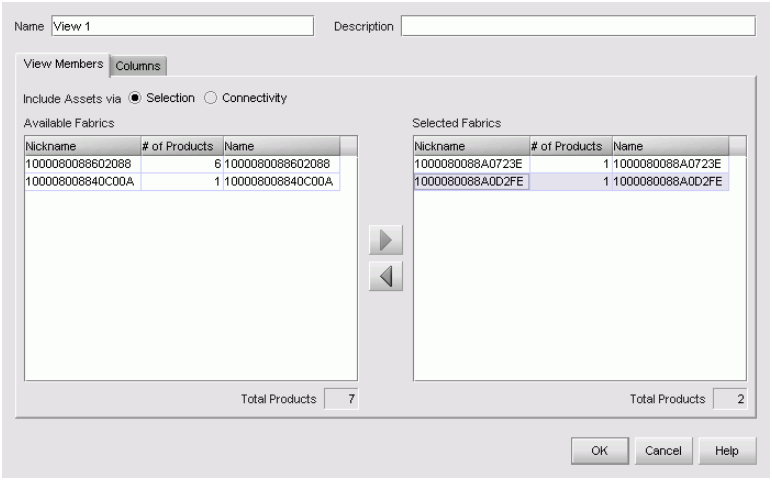


Figure 33: Edit View dialog box

2. Edit information as necessary. See "Creating a Customized View" on page 79 for detailed instructions.
3. Click **OK**.

Deleting a Customized View

To delete a customized view, perform the following:

1. Choose **View > Delete View**, then select the view you want to delete.

Note: Customized view settings reside on the appliance; if one user creates a view, all users who log on to the same appliance are able to select that view.

Selecting a Customized View

To select a customized view, perform the following:

1. Click the **View** tab and choose the view name from the menu.

Grouping on the Topology

To simplify management, devices display in groups, as shown in Figure 34. Groups are shown with background shading and are labeled appropriately. You can expand and collapse groups to easily view a large topology.

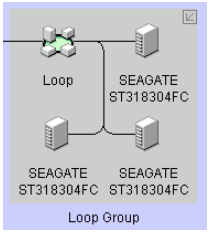


Figure 34: A Group on the Physical Map

Note: "Fabric" groups may not be true fabrics, but zonable fabrics are true fabrics. Fabric groups are a set of connected devices that may or may not be fabric devices.

Collapsing Groups

To collapse a single group on the topology, perform one of the following:

- Double-click the icon at the top right-hand corner of the group on the topology ( ).
- Double-click in the group, but not on a device.
- Right-click in a group, but not on a device, and choose **Collapse**.

To collapse all groups on the topology by one level, click the **Collapse** icon on the toolbox ( ).

Expanding Groups

To expand a group on the topology, perform one of the following:

- Double-click on the group icon.

- Right-click the group icon and choose **Expand**.

To expand all groups on the topology by one level, click the **Expand** icon on the toolbox ( ).

Customizing the Product List

You can customize the Product List to display only the data you need by creating views that display certain fabrics or by displaying different levels of detail on the Product List. This section provides instructions for customizing the Product List.

Adding a Column to the Product List

You can define new Product List columns to customize a view. This enables you to further customize the Product List to display pertinent device and port information.

1. You can add Product List columns to a new or an existing view using one of the following methods:
   - Choose **View > Create View**. The Create View dialog box displays, as shown in Figure 31 on page 80.
   - Choose **View > Edit View**, then select the view you want to edit. The Edit View dialog box displays, as shown in Figure 33 on page 82.
2. Click the **Columns** tab. The Create View dialog box with the Columns tab displays, as shown in Figure 32 on page 81.
3. Click **Add**. The Create Column dialog box displays, as shown in Figure 35.

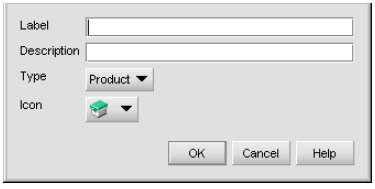


Figure 35: Create Column dialog box

4. Enter a label in the **Label** field.
5. Enter a description in the **Description** field.
6. Choose whether the column displays information about products or ports from the **Type** drop-down list.
7. Choose an icon to display in the column from the **Icon** drop-down list.

8. Click **OK**.
9. Highlight the column from the **Available Columns** table and click the right arrow button to display the new column in the Product List. The column name moves to the **Selected Columns** table.
10. Click **OK**. The new column displays in the Product List.

Changing a Column on the Product List

You can edit labels, definitions, information, and icons of existing Product List columns.

1. You can edit Product List columns to a new or an existing view using one of the following methods:
   - Choose **View > Create View**. The Create View dialog box displays, as shown in Figure 31 on page 80.
   - Choose **View > Edit View**, then select the view you want to edit. The Edit View dialog box displays, as shown in Figure 33 on page 82.
2. Click the **Columns** tab. The Create View dialog box with the Columns tab displays, as shown in Figure 32.
3. Click **Change**. The Edit Column dialog box displays, as shown in Figure 36.

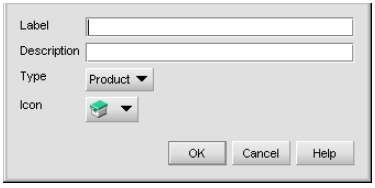


Figure 36: Edit Column Dialog Box

4. Edit the column properties as necessary.
5. Click **OK**.
6. To view the edited column in a customized view, follow the instructions in "Editing a Customized View" on page 82.

Removing a Column from the Product List

You can remove unused Product List columns in a customized view.

1. You can edit Product List columns to a new or an existing view using one of the following methods:

— Choose **View > Create View**. The Create View dialog box displays, as shown in Figure 31 on page 80.

— Choose **View > Edit View**, then select the view you want to edit. The Edit View dialog box displays, as shown in Figure 33 on page 82.

2. Click the **Columns** tab. The Create View dialog box with the Columns tab displays, as shown in Figure 32.
3. Make sure the column you want to remove displays in the **Available Columns** table. To move a column to the **Available Columns** table, highlight it in the **Selected Columns** table and click the left arrow button.
4. Highlight the column you want to remove.

Note: When you click **Remove**, the column definition is deleted without confirmation.

5. Click **Remove**.

Viewing Levels of Detail on the Product List

You can view different levels on the Product List.

Viewing All

To display all information on the Product List:

1. Click the **View All** tab.
2. Choose **Levels > All Levels**.

Viewing Only Products

To display only products on the Product List:

1. Click the **View All** tab.
2. Choose **Levels > Products Only**.

Zooming In and Out of the Topology

You can zoom in or out of the topology to see products and ports.

Zooming In

To zoom in on the Physical Map, use one of the following methods:

1. Click the zoom-in icon ( ) on the toolbox.

   or

1. Choose **View > Zoom**. The Zoom dialog box displays, as shown as Figure 37.

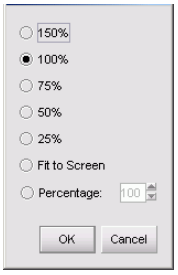


Figure 37: Zoom dialog box

2. Choose a zoom percentage.
3. Click **OK**.

Zooming Out

To zoom out of the Physical Map, use one of the following methods:

1. Click the zoom-out icon ( ) on the toolbox.

   or

1. Choose **View > Zoom**. The Zoom dialog box displays, as shown as Figure 37.
2. Choose a zoom percentage.
3. Click **OK**.

Showing Levels of Detail on the Physical Map

You can view different levels of detail on the Physical Map, making SAN management easier. To change the view of the physical map, perform the following:

1. Choose **View > Show** and then choose one of the available view options.

Turning Flyovers On or Off

Flyovers display when you place the cursor on a product. They provide a quick way to view a product's properties. To turn flyovers on or off, perform the following:

1. Choose **View > Enable Flyover Display** and then choose **On** or **Off**.

Exporting and Importing

The import and export features are important functions of the application. You can import and export data for many reasons, including to communicate issues to the support center and to capture network status.

Note: Currently, you can only export to and import from the same releases of the application (for example, export from release 8.0 and import to release 8.0).

Importing a file imports the Physical Map, the status icons, the user properties, and the discovered properties as they were set at the time of the export.

Exporting Data

You can export data to disk and to email.

1. Choose **SAN > Export**. The Export dialog box displays, as shown in Figure 38.

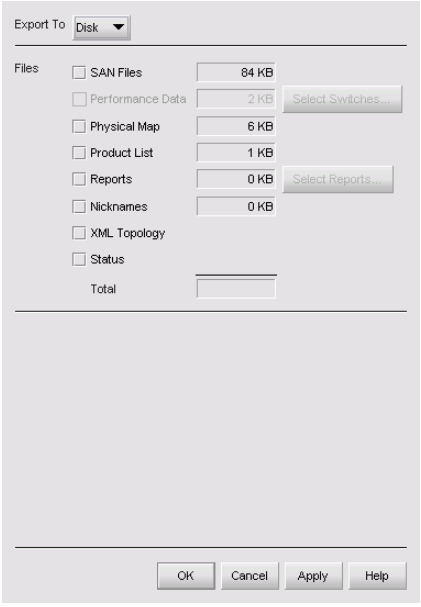


Figure 38: Export dialog box

2. Choose one of the following options from the **Export To** drop-down list:

— **Disk**—Saves the exported files to the disk in `<Install_Home>\Client\Data\san<date>\san*.zip`.

— **EMail**—Mails the exported files as an e-mail attachment directly from the application.

3. Choose the types of files that you want to export.

Note: Some file types may not be available based on the export destination you selected in the previous step.

— **SAN Files**—Exports the SAN files.

— **Physical Map**—Exports the Physical Map, or topology.

— **Performance Data**—Exports the performance data. This is an optional feature. Contact your sales representative to purchase this module. If you choose **Performance Data**, you can choose what switches to export data on by clicking **Select Switches**. The Select Switches dialog box displays, as shown in Figure 39.

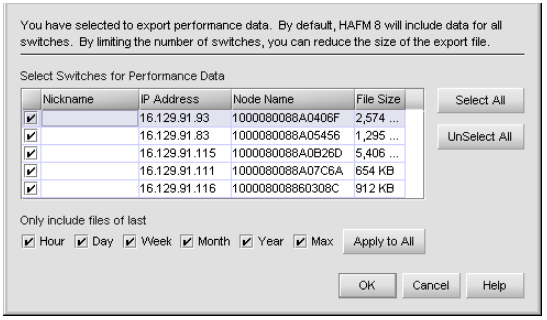


Figure 39: Select Switches dialog box

— **Product List**—Exports the Product List in tab-delimited format. To view the product list in table format, open it in Microsoft® Excel.

— **Reports**—Exports SAN reports.

— **Nicknames**—Exports nicknames.

— **XML Topology**—Exports description of all fabric topologies in XML format, including online and persisted product and connection information.

— **Status**—Exports SAN status data used by technical support.

4. If you are exporting to disk, skip to step 6. Otherwise, continue to step 5.
5. If you are exporting to email, enter information in the following fields:
   - **Mail To**—Enter the recipient's e-mail address.
   - **Mail List**—Click to select from a list of e-mail addresses.
   - **From**—Enter your email address.
   - **Subject**—Enter a subject for the e-mail message.
   - **Message**—Enter content for the e-mail message.
6. Click **OK** to export the files. If you exported to disk, a Confirmation message displays, as shown in Figure 40.

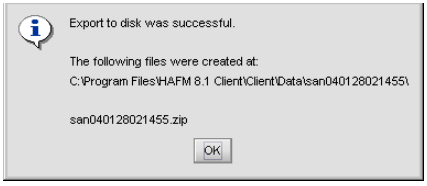


Figure 40: Export Confirmation message

7. Make a note of the file location and name and click **OK**.

Importing Data

You can choose to import the following information to the application:

Note: Importing files clear the Master Log of previous events.

Perform the following to import files:

1. Choose **SAN > Import**. The Import dialog box displays, as shown in Figure 41.

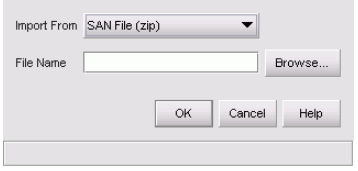


Figure 41: Import dialog box

2. Choose the type of file you want to import from the **Import From** list.
3. Enter the path and file name in the **File Name** field.

Note: The default path is: *<Install_Home>\ClientData\san<date>\san*.zip*. Be sure to select the san*.zip file for import. Importing the rep*.zip file causes errors.

---

4. Click **OK**. A message displays, stating that imported data replaced corresponding data on the appliance.
5. If you are sure you want to replace the data on the appliance, click **OK**. If you are importing a SAN file or a properties file, the client is logged out and the HAFM 8 Log In dialog box displays. Log back into the application.

Note: When discovery is on, the discovered SAN is replaced with the imported data. Only one SAN can be viewed at a time. For instructions about turning on discovery, see "Setting Up Discovery" on page 69.

Backing Up and Restoring Data

You can protect your SAN data by backing it up and then restore it as necessary. The HAFM appliance provides a platform for the Enhanced Base package of the *HAFM* application. This unit provides more memory for future product enhancements.

What is Backed Up?

The following data, contained in the `<Install_Home>\Call Home`, `<Install_Home>\Server`, and `<Install_Home>\Client` directories, are backed up to disk:

Note: `<Install_Home>` refers to the directory where the *HAFM* application is installed.

- All log files.
- Call-home configuration (including phone numbers and dialing options).
- Configuration data.
- License information.
- User launch scripts.
- User-defined sounds.
- All data exported through the **Export** option on the **SAN** menu.

Note: Firmware files are NOT backed up.

HAFM Appliance Backup and Restore

The HAFM appliance is backed up to a compact disk, rewritable (CD-RW). As long as a CD-RW disk remains in the CD recorder drive of the appliance, critical data from the *HAFM* application is automatically backed up to the CD-RW disk when the data directory contents change or when you restart the *HAFM* application.

Restoring Data

Backing up data takes some time. Wait about 45 minutes after making a configuration change before restoring from the backup files to ensure that all your changes are included in the backed up files. To restore data to the appliance platforms, follow these instructions:

1. Reinstall the application, if necessary.
2. To restore data to the application, copy the three folders from the CD-RW disk (`X:\Backup\` directory) and paste them in `C:\Program Files\<Install_Home>` directory. You are asked if you want to overwrite the existing files; click **Yes**.
3. On the HAFM appliance, open the *HAFM* application.
4. Choose **SAN > Import**. The Import dialog box displays, as shown in Figure 41.
5. Choose **SAN File (zip)** from the **Import From** drop-down list.
6. Click **Browse**. The Browse dialog box displays.

Note: Imported data replaces the corresponding data on the appliance, including log entries. If you want to keep the data on the appliance, perform an export before importing the new data. See "Exporting Data" on page 89 for instructions.

---

7. Select the file from the directory below and click **Open**.

   ```
   <Install_Home>\Server\Data\Backup\bkp(date and time)\bkp(date and time).zip
   ```

8. Click **OK** on the Import dialog box. A message displays stating that imported data replaces corresponding data on the appliance.
9. If you are sure you want to replace the data on the appliance, click **OK**. The client is logged out and the HAFM 8 Log In dialog box displays. For instructions on logging into HAFM, see "Accessing HAFM" on page 47.

Configuring SAN Products and Fabrics

3

This chapter provides instructions for configuring products and fabrics and setting up trap forwarding.

Managing Products

You can use the application to manage discovered products. You can search for a product, change its properties, and perform other configuration and maintenance tasks.

Opening a Product's Element Manager

You can open an Element Manager to manage switches and directors directly from the application.

Opening the Element Manager from the Interface

To open an Element Manager from the user interface, perform one of the following steps:

- Right-click a product icon and choose **Element Manager**.
- Double-click a product icon.

Note: If you encounter problems, ensure that only one copy of the application is being used to monitor and manage the device. Only one copy of the application should be used to monitor and manage the same devices in a subnet.

Opening the Element Manager from the Command Line

To open an Element Manager, you can use a script that is included with the application. In order to do this, the appliance must be running and the product must be discovered.

1. Open the script `<Install_Home>\bin\HAFM_ElementMgr.bat` using a text editor.
2. Under the heading, "rem HAFM Element Manager", find the line that begins:

   ```
   ...ElementManagerStandAlone -s ServerIp -p ProductIp -u UserName
   -pw Password
   ```

3. Enter information for the following parameters, ensuring that there are spaces between the options:
   - ServerIp: Appliance's IP address
   - ProductIp: Switch's or director's IP address
   - UserName: User login name

- Password: User password

Example

```
...ElementManagerStandAlone -s 172.16.9.10 -p 172.16.9.211 -u
Administrator -pw password
```

4. Save and close the file.
5. Run the script by double-clicking the file or entering the script name at a DOS prompt.
6. In case of errors, verify that the appliance is on and that the switch or director you are trying to access is being discovered.

Searching for Products in a SAN

You can search a discovered SAN for a specific product by its properties, such as name or IP address.

1. Enter the search parameter in the **Search** field on the toolbar, as shown in Figure 42.

Figure 42: Search Box

2. Click the up or down arrow to search forwards or backwards through the Physical Map.
3. Click **Search** to find each product.

Note: When the application finds a product on the Physical Map, it highlights the product on the Physical Map as well as on the Product List.

Changing Product Properties

You can change some of the properties for online products.

Note: This process does not change the configuration of the product. It only changes the information that is stored on the local appliance.

1. Right-click a product icon and choose **Properties**. The Properties dialog box displays, as shown in Figure 43.

Figure 43: Properties dialog box

Note: If the product you selected is offline, you are not be able to edit this information.

2. Edit information as necessary.
3. Click **OK**.

Determining a Product's Operational Status

You can determine a product's operational status by looking at the Physical Map or the Product List. On both the Physical Map and the Product List, you can determine a product's operational status by looking at the associated icons, as shown in Table 5.

Table 5: Product Status Icons

Icon	Status
No icon	Operational
	Degraded
	Failed
	Unknown/Offline

To see a list of all products requiring attention, click the Attention Indicator icon () on the Status bar at the bottom of the main window. The Service Request dialog box displays the names and IP addresses of devices needing attention. Click a product name hyperlink to jump to the product on the Physical Map. The list updates dynamically.

Showing Routes Between Two End-Products

Note: This feature is only available for fabrics consisting solely of HP M-series products.

You can use the Show Route feature to view the path that Fibre Channel frames must take between two end-products in a multiswitch fabric. Only one route can be shown at a time within the same fabric. If you intend to show a different route within the same fabric, the previous route is automatically hidden.

Requirements

To view the route between two products, the following conditions must be met:

- All switches or directors in the route must be managed by the application and attached to the same appliance.
- All switches or directors in the route must be Director 2/64, Director 2/140, Edge Switch 2/32, Edge Switch 2/16, or Edge Switch 2/24 models and must be running firmware version 1.3 or higher.
- All attached products in the route must be in the same zone.

Procedure

To show the route for two specific ports on the end nodes, perform the following:

1. In the Product List, click the **+** symbol next to a switch product icon to expend and see the attached nodes.
2. Right-click a node and select **Show Route.** The Show Route dialog box displays, as shown in Figure 44.

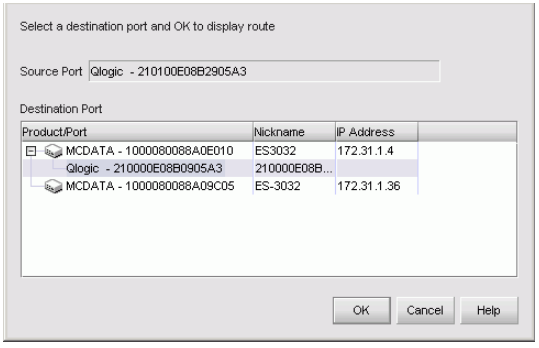


Figure 44: Show Route dialog box

3. Select a destination port from the **Destination Port** table.
4. Click **OK**. The route between the ports displays on topology, as shown in Figure 45.

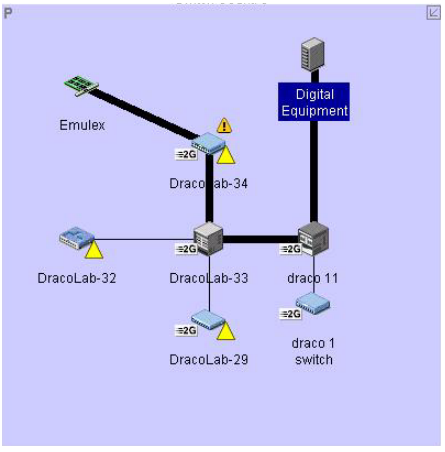


Figure 45: Show Route example

Hiding Routes Between Two End-Products

Note: This feature is only available for fabrics consisting solely of HP M-series products.

You can use the Hide Route feature to hide routes that Fibre Channel frames must take between two end-products in a multiswitch fabric. You must show routes before you can hide routes. See "Showing Routes Between Two End-Products" on page 99 for instructions on showing routes.

To hide the route, perform the following:

1. Right-click the route (line between end-nodes) or the fabric that includes the route you want to hide and choose **Hide Route**.

Viewing Properties of Routes Between Two End-Products

To view the properties of a route, perform the following:

1. Right-click the route and choose **Properties**. The Route Properties dialog box displays, as shown in Figure 46.

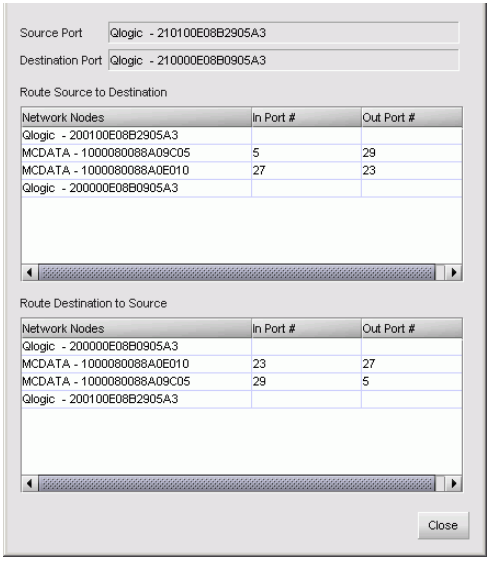


Figure 46: Route Properties dialog box

2. Review the source and destination ports, as well as route details.
3. Click **Close**.

Changing a Fabric's Properties

To view and change a fabric's properties, perform the following:

1. Right-click a fabric icon or the background of an expanded fabric and choose **Properties**. The fabric's **Properties** dialog box displays, as shown in Figure 47.

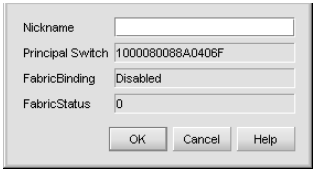


Figure 47: Fabric Properties dialog box

2. View the fabric's information and edit the nickname, if desired.

Note: Once you assign a nickname, you cannot delete it and leave it blank.

3. Click **OK**.

Configuring Enterprise Fabric Mode

The **Enterprise Fabric Mode** option is available on the **Configure** menu. This option automatically enables features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. When Enterprise Fabric Mode is enabled, each switch in the fabric automatically enforces a number of security-related features including Fabric Binding, Switch Binding, Insistent Domain IDs, Domain Register for State Change Notifications (RSCNs), and Rerouting Delays.

About Enterprise Fabric Mode

Activating Enterprise Fabric Mode enables the following:

- **Fabric Binding**—Allows or prohibits switches from merging with a selected fabric.
- **Switch Binding**—This feature, enabled through a product's Element Manager, allows or prohibits switches from connecting to switch E_Ports and products from connecting to F_Ports.
- **Rerouting Delay**—This feature, enabled through a product's Element Manager, ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.
- **Domain RSCNs**—This feature, enabled through a product's Element Manager, indicates that an event occurred to a switch in a fabric. The only cause would be a switch entering or leaving the fabric. Notifications are sent fabric-wide and are not constrained by a zone set. Domain RSCNs are not sent between end-products.
- **Insistent Domain ID**—This feature, enabled through a product's Element Manager, sets the domain ID as the active domain identification when the fabric initializes. If Insistent Domain ID is enabled, the switch isolates itself from the fabric if the preferred Domain ID is not assigned as the switch's Domain ID.

Setting Enterprise Fabric Mode

To enable or disable Enterprise Fabric Mode for a fabric, perform the following:

1. Choose **Configure > Enterprise Fabric Mode**. The Enterprise Fabric Mode dialog box displays, as shown in Figure 48.

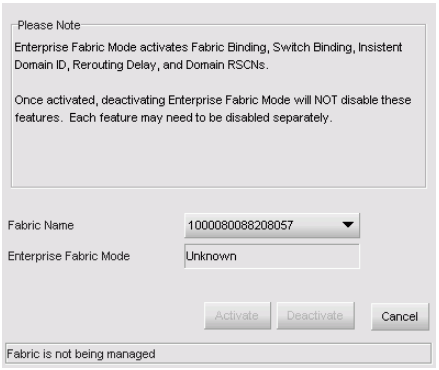


Figure 48: Enterprise Fabric Mode dialog box

2. Choose the fabric for which you want to configure Enterprise Fabric Mode from the **Fabric Name** drop-down list.
3. The fabric's current status displays in the **Enterprise Fabric Mode** field.
4. To activate Enterprise Fabric Mode on the selected fabric, click **Activate**.

   To deactivate Enterprise Fabric Mode on the selected fabric, click **Deactivate**.

Note: You must be managing the fabric in order to deactivate Enterprise Fabric Mode.

Configuring Fabric Binding

The fabric binding feature enables you to configure whether switches can merge with a selected fabric. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Note: You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding.

Enabling Fabric Binding

Fabric Binding is enabled through the Fabric Binding dialog box. After you have enabled Fabric Binding, use the **Fabric Membership List** to add switches that you want to allow into the fabric.

1. Choose **Configure > Fabric Binding**. The Fabric Binding dialog box displays, as shown in Figure 49.

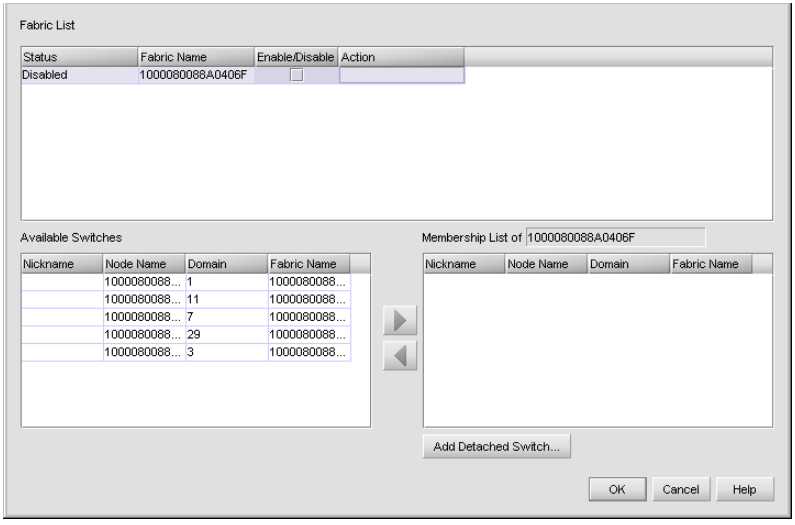


Figure 49: Fabric Binding dialog box

2. Click the **Enable/Disable** checkbox for fabrics for which you want to configure fabric binding in the **Fabric List** table. If SANtegrity Binding is not installed, a message box displays, as shown in Figure 50.

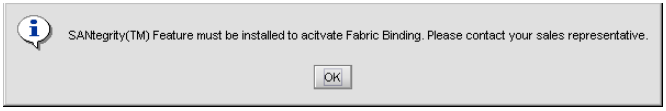


Figure 50: SANtegrity feature message

3. Click **OK**.
4. Click **OK**.
   or
   If you want to add switches to the membership list, see "Adding Switches to the Fabric Binding Membership" on page 106 for instructions.

Adding Switches to the Fabric Binding Membership

Once you have enabled Fabric Binding (see "Enabling Fabric Binding" on page 105), you can add and remove switches from the membership list.

1. Add switches to the selected fabric's Fabric Membership List (FML) by selecting the switches from the **Available Switches** table and clicking the  button to move the switches to the **Membership List** table.
2. Click **Add Detached Switch** to add a switch that does not have physical connection to the fabric. The Add Detached Switch dialog box displays, as shown in Figure 51.

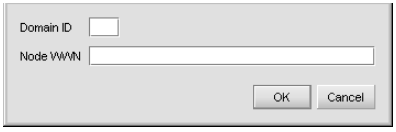


Figure 51: Add Detached Switch dialog box

   a. Enter the domain ID in the **Domain ID** field.
   b. Enter the node World Wide Name in the **Node WWN** field.
   c. Click **OK**.

Persisting and Unpersisting Fabrics

Persisting fabrics takes a "snapshot" of the current products and connections in the fabric as a reference point for comparison to future fabric changes. You can export the topology, including persisted fabric information. See "Exporting Data" on page 89.

Note: If the fabric's principal switch changes, the new fabric must be manually persisted. Persistence does not follow the new fabric even if only one switch is removed from the original fabric. The principal switch should always be managed. Also, the principal switch must be a HP switch or director in order to manage the devices in the fabric.

Persisting a Fabric

To persist a fabric, perform one of the following:

- Highlight a fabric in the Physical Map or Product List, then choose **Configure > Persist Fabric**.
- Right-click the fabric in the Physical Map or Product List, then choose **Persist Fabric**.
- Highlight a fabric in the Physical Map or Product List, then click the **Persist Fabric** icon on the toolbar.

Unpersisting a Fabric

To unpersist a fabric, perform the following:

1. Highlight a fabric in the Physical Map or Product List, then choose **Configure > Unpersist Fabric**. A confirmation box displays, as shown in Figure 52.
   or
   Right-click the fabric in the Physical Map or Product List, then choose **Unpersist Fabric**. A confirmation box displays, as shown in Figure 52.

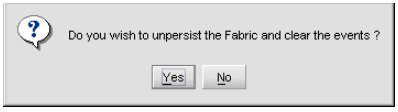


Figure 52: Unpersist Fabric confirmation box

2. Click **OK**.

Unpersisting a Single Product

You can unpersist a single product in a persisted fabric if the product is no longer part of the fabric. When a product is unpersisted, the connections associated with that product are also removed. The persisted fabric's data is updated with the changes.

To unpersist a product, perform the following:

1. Right-click the product in the Physical Map or Product List, then choose **Unpersist Fabric**. A confirmation box displays, as shown in Figure 52.
2. Click **OK**.

Graphic Indicators Related to Persisted Fabrics

There are various ways to determine the status of persisted fabrics and persisted products. Real-time changes to the fabric display on the Physical Map and the Product List and are listed in the Fabric Log.

Determining a Persisted Fabric's Status

The fabric's status is reflected by the green circle indicator that displays on the fabric icon on the Physical Map and in the Product List (Figure 53 and Figure 54, respectively). See "Product Status Icons" on page 272 for a list of status icon definitions.

Figure 53: Persisted Fabric icon on Physical Map

Figure 54: Persisted Fabric icon on Product List

You can also determine changes to the persisted fabric through the Fabric Log. To display the log, perform the following:

1. Highlight a persisted fabric in the Physical Map or Product List and choose **Monitor > Logs > Fabric Log**. For more details on the Fabric Log, see "Event Monitoring" on page 114.

Determining Status of a Product in a Persisted Fabric

When a product is added to a persisted fabric, it displays with a "plus" icon, as shown in Figure 55.

Figure 55: Product Added to Persisted Fabric

When a product is removed from a persisted fabric, it displays with a "minus" icon, as shown in Figure 56.

Figure 56: Product Removed from Persisted Fabric

Determining the Status of Connections in a Persisted Fabric

If more than one connection exists between products and all connections are disconnected, the connections change to yellow, dashed lines. If one or some of the connections are disconnected (but not all), the enabled connections display as black lines and the disabled connections display as yellow, dashed lines with an interswitch link (ISL) alert, as shown in Figure 57.

To remove an ISL alert, perform the following:

1. Right-click the connection and choose **Clear ISL Alert(s)**. If an ISL is added, the ISL displays as a black line.

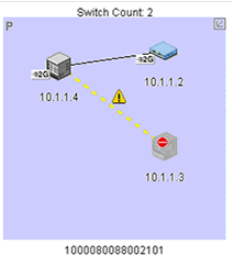


Figure 57: Removed Connection in a Persisted Fabric

Clearing ISL Alerts

To clear a single ISL alert, perform the following:

1. Right-click the ISL and choose **Clear ISL Alert(s)**.

To clear all ISL alerts, perform the following:

1. Choose **Edit > Clear All ISL Alerts**.

Merging Persisted Fabrics

When you merge two persisted fabrics, the fabric whose principal switch is the principal switch in the merged fabric becomes the “real” fabric. It includes the switches of both fabrics in the Physical Map and the Product List. The other fabric becomes a “ghost” fabric.

On the Physical Map, the ghost fabric displays its original products with “minus” symbols, as shown in Figure 56. On the Product List, the fabric displays as offline and no products display under the fabric. The ghost fabric is not updated and the Fabric Log is reset after the fabrics merge.

Splitting Persisted Fabrics

When you split persisted fabrics, the principal switch determines which fabric is mapped to the persistent fabric. The fabric that includes the principal switch is mapped to the persistent fabric.

Layout Changes in Persisted Fabrics

When you move a product in a persisted fabric’s topology, the new positions are stored on the client. If you log in to the appliance from a different client, you lose the layout of the products if the fabric is not persisted with the layout changes.

Finding Devices in a Persisted Fabric

When a product is removed from a persisted fabric, it displays a “ghost” image with a minus icon, as shown in Figure 56.

To find a product that is removed from a persisted fabric, perform the following:

1. Right-click the icon and choose **Find Product**. The focus jumps to the online item that corresponds to the “ghost” image from the original fabric.

Configuring Trap Forwarding

Trap forwarding is the process by which you can configure the application to send SNMP traps to other computers. To correctly configure trap reporting, you must configure the target computer’s IP address and SNMP ports in the Configure Trap Forwarding dialog box.

Configuring Trap Forwarding

1. Choose **Monitor > Trap Forwarding**. The Configure Trap Forwarding dialog box displays, as shown in Figure 58.

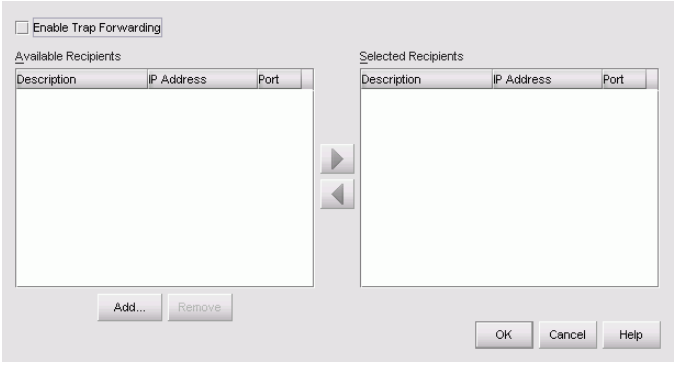


Figure 58: Configure Trap Forwarding dialog box

2. If necessary, add or remove trap recipients. See “Adding Trap Recipients” on page 112 and “Removing Trap Recipients” on page 112 for instructions.
3. Highlight the recipient from the **Available Recipients** table and add it to the **Selected Recipients** table by clicking the button.
4. Choose the **Enable Trap Forwarding** option to forward all traps received by the application to the recipients listed in the **Selected Recipients** table.

5. Click **OK**.

Adding Trap Recipients

1. Choose **Monitor > Trap Forwarding**. The Configure Trap Forwarding dialog box displays, as shown in Figure 58.
2. Click **Add**. The Add Trap Recipient dialog box displays, as shown in Figure 59.

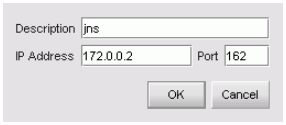


Figure 59: Add Trap Recipient dialog box

3. Enter a description of the trap recipient in the **Description** field.
4. Enter the trap recipient's IP address in the **IP Address** field.
5. Enter the trap recipient's TCP/IP port number in the **Port** field.
6. Click **OK**.
7. Click **OK**.

Removing Trap Recipients

1. Choose **Monitor > Trap Forwarding**. The Configure Trap Forwarding dialog box displays, as shown in Figure 58.
2. Highlight the recipient you want to remove in the **Available Recipients** table.
3. Click **Remove**.
4. Click **OK**.

Monitoring SAN Products

4

This chapter provides instructions for monitoring SAN products using the application.

Event Monitoring

The application provides a variety of logs through which you can monitor the SAN. The event log file name is *event.log*.

You can view all events that take place in the SAN through the Master Log at the bottom of the main window. You can also view a specific log by choosing **Monitor > Logs**, then choose an option from the menu. The available logs include:

- **Audit Log**—Displays a history of user actions performed through the application (except log in/log out).
- **Event Log**—Displays errors related to SNMP traps and client-server communications.
- **Session Log**—Displays the users who have logged in and out of the appliance.
- **Product State Log**—Displays operational status changes of managed products.

The application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. See "Using Event Notification Features" on page 118 for details.

For information about the Master Log interface, fields, and icons, see "Master Log" on page 37.

Viewing Logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only login/logout events (session events), open a specific log through the View Logs dialog box.

To view a log, perform the following:

1. Choose **Monitor > Logs**, then choose one of the options. The View Logs dialog box displays, as shown in Figure 60.

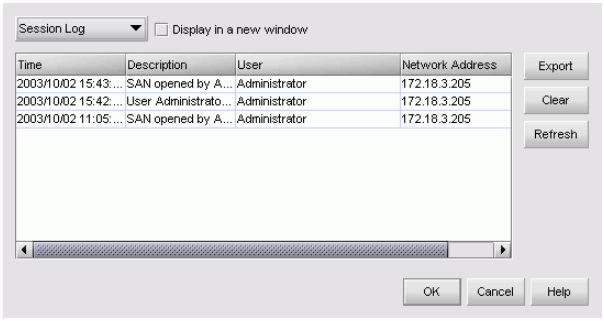


Figure 60: View Logs dialog box

- **To view a different log**, choose a log from the drop-down list.
- **To view multiple logs simultaneously**, choose the **Display in a new window** check box and choose another log from the drop-down list.
- **To clear the log**, click **Clear**.
- **To refresh the log**, click **Refresh**.
- **To export log entries**, see "Exporting Log Data" on page 115.

2. Click **OK** to close the dialog box.

Exporting Log Data

You can export HAFM log data in tab-delimited format. This feature is useful for providing the data to a third-party or including it in a report.

1. Choose **Monitor > Logs**, then choose one of the options. The View Logs dialog box displays, as shown in Figure 60.
2. Click **Export**. The Save dialog box displays.
3. Browse to the folder where you want to save the file. Type a file name in the **File Name** field.
4. Click **Save**. The file is exported in tab-delimited format. To view it in table format, open the file in Microsoft Excel.

Filtering Events in the Master Log

You can filter the events that display in the Master Log on the main window. For more information, see “Master Log” on page 37.

1. Click the **Define** link on the Master Log. The Define Filter dialog box displays, as shown in Figure 61.

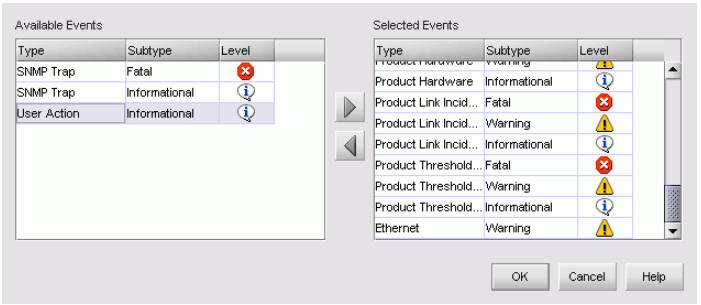


Figure 61: Define Filter dialog box

2. Highlight the event from the **Available Events** table to include an event type in the filter and click the right arrow button.
3. Highlight the event from the **Selected Events** table to exclude an event type from the filter and click the left arrow button.
4. Click **OK**.

Copying Log Entries

You can copy data and column headings from logs to other applications. Use this function to analyze or store the data using another tool.

Note: When using the View Logs dialog box, you can only copy one row at a time. To copy multiple rows of data, copy the data from the Master Log on the main window.

Copying Rows

To copy rows from logs to other applications, perform the following:

1. Highlight the row(s) you want to copy in the log window.
   - To select contiguous rows, highlight the first row you want to copy and **Shift**-click in the last contiguous row you want to copy.

- To select non-contiguous rows, highlight the first row you want to copy and **CTRL**-click every additional row you want to copy.

2. Press **CTRL+C** to copy the selected information on the clipboard in tab-delimited format.
3. Open the application you want to paste the data into and click where you want to paste the data.
4. Press **CTRL+V** (or use the **Paste** command from the other application). All data and column headings are pasted.

Copying the Entire Master Log

To copy the entire Master Log, perform the following:

1. Click in the list on the Master Log window.
2. Choose **Edit > Select All** (**CTRL+A**). All Master Log rows are selected.
3. Press **CTRL+C** to copy the selected information in tab-delimited format.
4. Open the application you want to paste the data into and click where you want to paste the data.
5. Press **CTRL+V** (or use the **Paste** command from the other application). All data and column headings are pasted.

Using Event Notification Features

The application records the SAN events in the Master Log. You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN. You can also configure products to “call home” for certain events, notifying the service center of product problems.

Configuring Email Notification

You can configure the application to send notification of events to users.

1. Choose **Monitor > Event Notification > Email**. The **Email Event Notification Setup** dialog box displays, as shown in Figure 62.

Figure 62: Email Notification Setup dialog box

2. Choose **Enable Email Event Notification** to enable e-mail notification.
3. Enter the IP address or the name of the SMTP mail server in the **E-mail Server** field.
4. Enter the recipient’s e-mail address in the **Reply** field.
5. Click **Test Email** to test the e-mail server. A message displays indicating if the server was found.

   If the server was not found, verify that the server address was entered correctly and that the server is running.
6. Enter the length of time the application should wait between notifications in the **Interval** field.

   Notifications are combined into a single e-mail and sent at each interval setting. An interval setting of zero causes notifications to be sent immediately.

Note: Setting too short of an interval can cause the recipient's e-mail inbox to fill VERY quickly.

7. Click **User List** to specify which users receive e-mail notifications. The HAFM 8 Server Users dialog box displays.
8. Choose the check box in the **Email** column for each user.
9. Click **OK**.

Configuring Call Home Notification

By configuring the call home feature, you enable the appliance to automatically dial-in to a support center to report system problems. To set up the call home feature, you must first specify the support center information through the call home configurator and then enable the call home feature through the *HAFM* application. If you are upgrading from a previous release of the application, all of your call home settings are preserved.

Part 1: Specifying Support Center Information

Follow these instructions only if you are using a U.S.-based call home provider. If you are configuring call home using a provider outside the U.S., contact your Customer Support representative.

1. When you installed the *HAFM* application, a **Call Home Configuration** icon was added to your desktop. Double-click this icon. The Call Home Configuration dialog box displays, as shown in Figure 63.

Figure 63: Call Home Configuration dialog box (for U.S. installations)

2. Enter the phone number for the primary attention server located at the call center in the **Call Center Phone Number** field. Be sure to include all the information necessary, including country codes, area codes, and any prefix required to access an outside line.
3. Enter the phone number where the local server can be reached in the **Local Phone Number** field. Include all the information necessary, including country codes and area codes.

4. Click **OK**. A message may display.
5. Click **OK**.
6. Continue to "Part 2: Enabling Call Home Notifications" on page 120.

Part 2: Enabling Call Home Notifications

1. Choose **Monitor > Event Notification > Call Home**. The Call Home Event Notification dialog box displays, as shown in Figure 64.

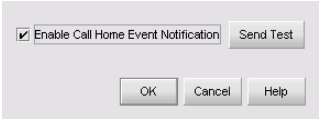


Figure 64: Call Home Event Notification dialog box

2. Choose **Enable Call Home Event Notification** to enable call home notification.
3. Click **Send Test** to test the call home function.

   A fake event is sent to the service center and you are asked to verify that the service center received the notification. If the server was not found, verify that the server address was entered correctly and that the server is running.
4. Click **OK**.

To verify call home settings, click the Call Home icon ( ) on the Status Bar.

Enabling Ethernet Events

An Ethernet event occurs when the Ethernet link between the appliance and the managed product is lost. You can configure the application to send notification of Ethernet events.

1. Choose **Monitor > Ethernet Event**. The Configure Ethernet Event dialog box displays, as shown in Figure 65.

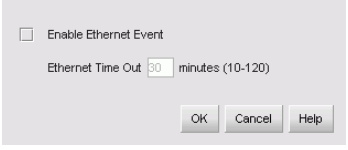


Figure 65: Configure Ethernet Event dialog box

2. Choose **Enable Ethernet Event** to be notified when the Ethernet link between the appliance and the managed product is lost.

3. Enter the length of time the application should wait before notifying you of the event in the **Ethernet Time Out** field.
4. Click **OK**.

Creating Reports

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SAN's architecture, or archive them for future reference.

The following report types are available:

- **Product List—**Lists the Product List, which has detailed information about the products in the SAN.
- **Operating Status Change**—Lists status change for products in the SAN, including the number of products online and offline, the product with the most downtime, and details about each product's status.
- **Performance Data—**Displays the performance data. The Performance Module is an optional feature. Contact your sales representative to purchase this module.
- **Physical Map**—Displays a graphic of the SAN's topology.
- **Port Usage**—Lists the number of used ports in the SAN as well as detailed usage information for each port.
- **Fabric Ports**—Lists fabric details including port and director utilization and individual product data.

Generating and Printing Reports

You can generate various reports of the SAN. Generated reports are saved to `<Install_Home>\Server\Reports\`.

1. Choose **Monitor > Report > Generate**. The Select Template dialog box displays as shown in Figure 66.

Figure 66: Select Template Dialog Box

Note: You can also generate a report of the Physical Map by clicking the **Generate Reports** button (or **CTRL+G**) on the right-hand toolbox while viewing a discovered SAN.

2. Select the type(s) of reports you want to generate.
3. Click **OK**.
4. The generated reports will automatically display in the **HAFM 8 Reports** dialog box.
5. To print the report, click **Show in Browser** to display the selected report in your default Web browser.
6. Choose **File > Print** in the Web browser.

Note: Hyperlinks in reports are only active as long as the source data is available.

Viewing and Printing Reports

You can view reports through the application, or through an internet browser. Reports are stored in `<Install_Home>\Server\Reports\`.

From the **Monitor** menu, select **Report**, then **View**. The HAFM Reports dialog box displays as shown in Figure 67.

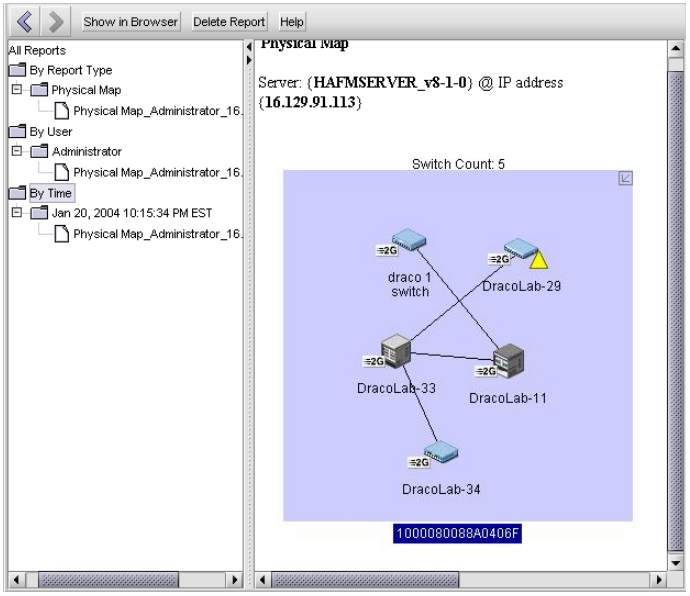


Figure 67: HAFM Reports Dialog Box

1. In the left-hand pane, select the report you want to view. If you don't see the report you want to view, generate it first by following the instructions in "Generating and Printing Reports" on page 122.

Note: Hyperlinks in reports will only be active as long as the source data is available.

2. Click the **Show in Browser** button to view the report in your Web default browser window.
3. Choose **File > Print** in the Web browser.
4. Click the **X** button in the upper right-hand corner of the HAFM 8 Reports window to close it.

Deleting Reports

You can delete reports using the View Reports dialog box.

1. From the **Monitor** menu, select **Report**, then **View**. The HAFM 8 Reports dialog box displays, as shown in Figure 67.

2. Select the report(s) you want to delete.

Note: Once you click **Delete Reports**, the report will be deleted without confirmation.

---

3. Click **Delete Reports**.
4. Click the **X** button in the upper right-hand corner of the HAFM 8 Reports window to close it.

Optional Features

5

This chapter provides detailed information on using, administering, and configuring optional HAFM features through *HAFM* applications. There are two types of features covered in this chapter:

- "Keyed" features, requiring feature keys to be purchased and enabled through the Configure Feature Key dialog box in the product's *Element Manager* application.
- Features not requiring feature keys themselves, but requiring that specific keyed features be enabled before they can be accessed through *HAFM* or *Element Manager* applications.

This chapter describes the following features:

Event Management Overview

This section provides an overview of the Event Management feature, as well as descriptions of the Event Management user interface.

Uses for Event Management

You can use Event Management to automate tasks that you perform on the SAN. You can configure the application to automatically perform many different functions using Event Management. Some examples of these functions or actions include:

- Sending an e-mail when events or errors occur.
- Generating reports at specific times or for specific reasons.
- Exporting data.
- Playing sounds to notify you of specific events.

Event Management Component Overview

Use the Event Management feature to automate SAN tasks by creating rules with triggers and actions.

About Triggers

When creating a rule, you need to specify triggers and actions. The two types of triggers, event and schedule triggers, are comprised of logically-related phrases, and each phrase is comprised of three parts:

- **Property**—A property is a variable for which you are setting values. For descriptions, see "Event Trigger Properties" on page 276.
- **Operator**—An operator is a logical or string function that you use to construct triggers and actions. For details, see "Trigger Operators" on page 129.
- **Value**—A user-defined value, such as time. For details, see "Values" on page 129.

Each rule can only have one type of trigger. In other words, each rule may have either an event or a schedule trigger; they may not be combined.

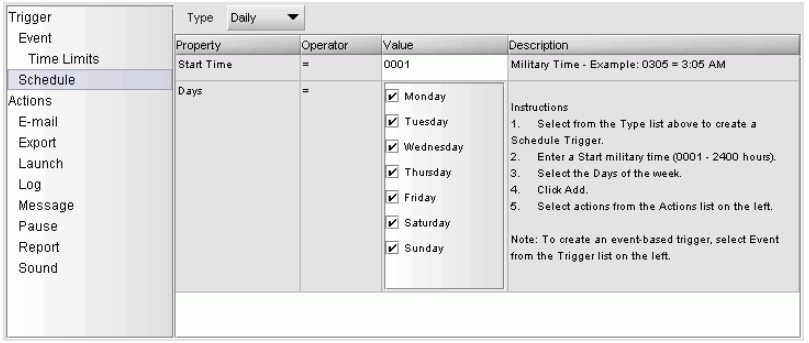


Figure 68: Trigger phrase development

Trigger Operators

Operators define the relationship between properties and their values. The list of available operators varies depending on whether the value can be a string or a number. The full list of operators is shown in Table 6.

Table 6: Trigger Operators

Operator	Value
==	Number
!=	Number
<	Number
<=	Number
>	Number
>=	Number
Contains	String
Does Not Contain	String
Starts With	String
Ends With	String

Values

Values are either presented in a list or entered by the user.

Phrase Operators

The phrases in the trigger area are related using these operators:

- AND
- OR
- AND NOT
- OR NOT

Each phrase, except the first one, starts with a logical operator. The default operator is AND.

About Event Triggers

Event triggers have the underlying concept of context. The context is the set of relevant properties that exist at the time an event takes place. You build the phrases (rows) and their logical relationships. The phrases filter all the event context properties to identify those events that you want to trigger the event.

Event triggers also allow you to set time limits so that the trigger only occurs if the event happens within a certain time and date range.

See "Event Trigger Properties" on page 276 for details on event type property descriptions.

About Schedule Triggers

Schedule triggers monitor the system clock and fire when the specified time and date conditions are met.

After selecting the schedule trigger, select a schedule type:

- Daily
- Weekly
- Monthly
- One Time
- Hourly

Note: Once you have chosen a type and added the first phrase, do not change types or you may lose your work.

Note: Once you have selected a trigger type, you can only choose options within that type to complete the trigger.

After selecting the category, you can specify whether all events in the category or some subset of events trigger the rule.

About Actions

You can configure multiple actions to be performed when the specified triggers are fired.

The following actions are available:

- **E-mail**—Send an e-mail to specified recipients.
- **Export**—Exports data.
- **Launch**—Launches the specified application using a script.
- **Log**—Adds an entry to the master log file and screen display.
- **Message**—Displays a message to all open clients.
- **Pause**—Inserts a pause between actions.
- **Report**—Generates a report.
- **Sound**—Plays a sound.

Note: You can specify macros for some actions by clicking in the **Value** column and then right-clicking and selecting an argument from the menu. See "Writing Event Management Macros" on page 284 for instructions.

Event Management Page Description

To view Event Management, click the **Event Management** tab on the main window of the application. All configured rules display. You can activate, deactivate, create, edit, copy, or delete rules on this page. You can also turn the Event Management feature on or off. See "Using Event Management" on page 133 for instructions on writing rules.

Table 7: Event Management Options

Field	Description
# column	Specifies the auto-assigned rule number.
Actions list	Lists the actions to be performed when the rule's triggers are met.
Activate button	Click to activate the selected rules.

Table 7: Event Management Options (Continued)

Field	Description
Active column	Specifies whether the rule is on.
Change button	Click to change the reset interval.
Copy button	Click to duplicate the selected rule.
Date Modified column	Lists the date and time that the rule was last edited.
Deactivate button	Click to deactivate the selected rules.
Delete button	Click to delete the selected rule.
Description field	Lists the description of the selected rule.
Description column	Specifies the user-defined rule description.
Edit button	Click to edit the selected rule.
Group column	Lists the group to which the rule belongs.
Name column	Specifies the user-defined rule name.
New button	Click to add a new rule.
OFF button	Click to turn the Event Management feature off.
ON button	Click to turn the Event Management feature on.
Trigger list	Lists the trigger for the selected rule.
User column	Specifies the last user to modify the rule.

Using Event Management

This section provides instructions for using the Event Management feature to automate tasks.

Specifying a Rule's Triggers

When you write a rule, you must begin by specifying a trigger that initiates an action. Triggers can be based on an event (for example, performance event), or on a schedule (for example, every day at 2 AM).

Adding an Event Trigger

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69.

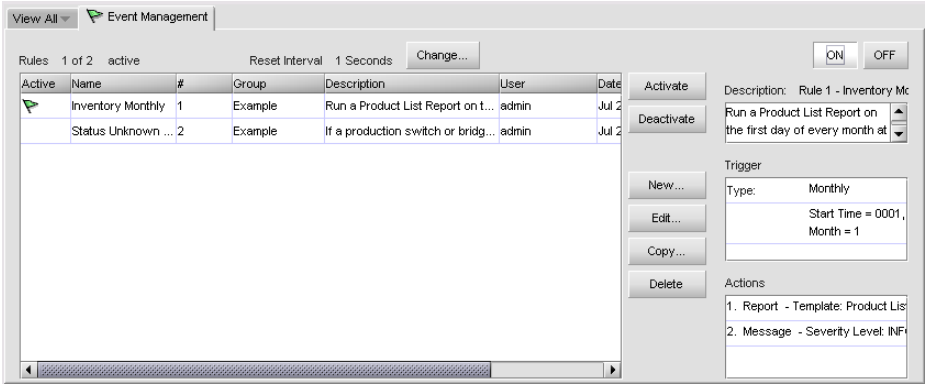


Figure 69: Event Management tab

2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.

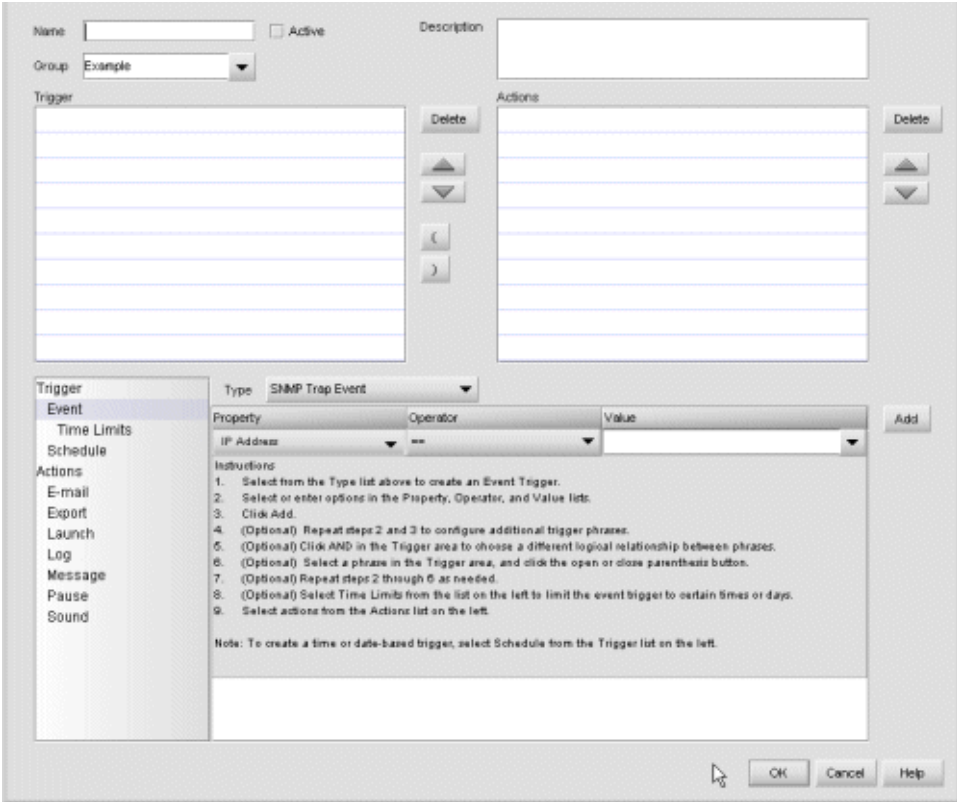


Figure 70: Add Rule dialog box

3. Enter a name for the rule in the **Name** field.
4. Choose or enter a group name in the **Group** field.
5. Choose the **Active** check box if you want to make the rule active after you are finished creating it.
6. Enter a description for the rule in the **Description** field.
7. Choose a type from the **Type** drop-down list.
8. Choose or enter data in the **Property**, **Operator**, and **Value** fields.
9. Click **Add**. The first line of the trigger you wrote displays in the **Trigger** table in the top half of the dialog box.
10. Repeat step 7 through step 9 to add additional phrases to the rule trigger.

11. Use the buttons to the right of the **Trigger** area to organize the syntax of the trigger.
    - Click the up and down arrows to move selected phrases up and down in the table.
    - Click **Delete** to remove selected rows from the table.
    - Click the parenthesis buttons to add parentheses to selected phrases.
    - To delete a parenthesis, highlight the parenthesis and click **Delete**.
12. Enter time limits for the event trigger, see "Specifying Time Limits for an Event Trigger" on page 135.
13. Choose an action from the **Actions** list at the bottom left of the dialog box. For help with adding specific actions, see "Event Management Component Overview" on page 128.
14. Enter the required information in the **Value** column for each listed parameter.
15. Click **Add**. The action you configured displays in the **Actions** area in the top half of the dialog box.
16. Repeat step 13 through step 15 to add more actions.
17. Use the buttons to the right of the **Actions** area to move the action phrases up or down.
    - Click **Delete** to remove selected rows from the table.
    - Click the up and down arrows to move selected actions up and down to change the order in which the actions are started.
18. Click **OK**.

Specifying Time Limits for an Event Trigger

Time limit triggers are used to specify times during which an event trigger should be fired. For example, you may specify that all offline events between 5PM and 8AM trigger e-mail message and log actions to take place. Thus, the application sends an e-mail to notify users of the event and adds a second, more detailed entry to the master log.

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.

3. Add an event trigger. See "Adding an Event Trigger" on page 133 for instructions.
4. Choose **Time Limits** from the **Trigger** list on the left to add a time limit to the rule. The **Time Limits** information displays, as shown in Figure 71.

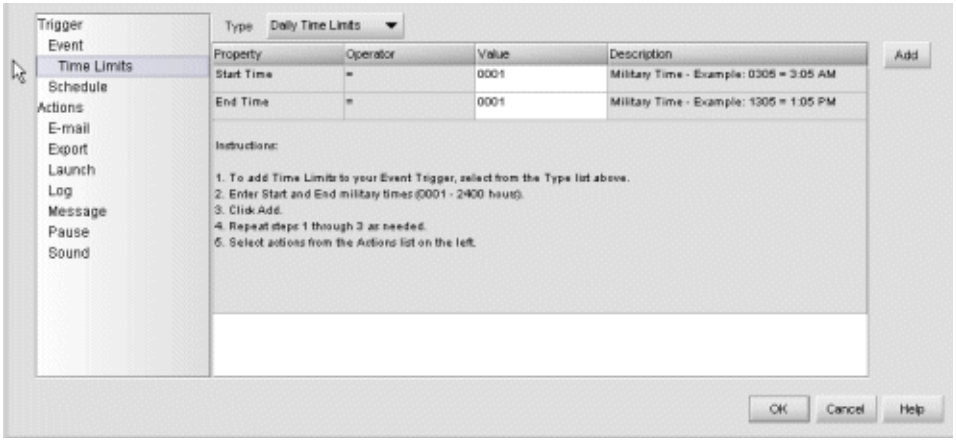


Figure 71: Add Rule dialog box (Time Limits)

5. Choose **Daily Time Limits** or **Weekly Time Limits** from the **Type** drop-down list.
   - If you selected **Daily Time Limits**: Enter the start time and end time (in military time format) in the **Value** fields and click **Add**.
   - If you selected **Weekly Time Limits**: Enter the start time and end time in (military time format) in the **Value** fields. Then, choose an option from the **Start Day** and **End Day** drop-down lists and click **Add**.
6. Click **Add**.
7. Add actions by selecting from the **Actions** list on the left. See "About Actions" on page 131 for instructions.

Adding a Schedule Trigger

You can add a schedule trigger to specify the time and date that an action should be performed.

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.

3. Enter a name for the rule in the **Name** field.
4. Choose or enter a group name in the **Group** field.
5. Choose the **Active** check box if you want to make the rule active after you are finished creating it.
6. Enter a description for the rule in the **Description** field.
7. Choose **Schedule** from the **Trigger** list at the bottom left of the dialog box. The **Schedule** information displays, as shown in Figure 72.

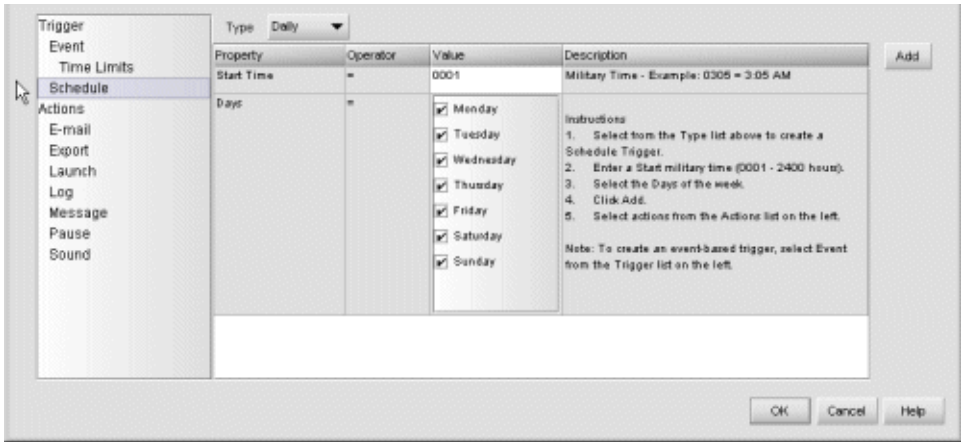


Figure 72: Add Rule dialog box (Schedule)

8. Choose a type from the **Type** drop-down list.
9. Choose or enter data in the **Value** field.
10. Click **Add**. The first line of the trigger you wrote displays in the **Trigger** table in the top half of the dialog box.
11. Repeat step 8 through step 10 to add additional phrases to the schedule trigger.
12. Use the buttons to the right of the **Trigger** area to organize the syntax of the trigger.
    - Click the up and down arrows to move selected phrases up and down in the table.
    - Click **Delete** to remove selected rows from the table.
    - Click the parenthesis buttons to add parentheses to selected phrases.
    - To delete a parenthesis, highlight the parenthesis and click **Delete**.

13. Choose an action from the **Actions** list at the bottom left of the dialog box. For help with adding specific actions, see "Event Management Component Overview" on page 128.
14. Enter the required information in the **Value** column for each listed parameter.
15. Click **Add**. The action you configured displays in the **Actions** area in the top half of the dialog box.
16. Repeat step 14 through step 15 to add more actions.
17. Use the buttons to the right of the **Actions** area to move the action phrases up or down.
    - Click **Delete** to remove selected rows from the table.
    - Click the up and down arrows to move selected actions up and down to change the order in which the actions are started.
18. Click **OK**.

Specifying a Rule's Actions

After specifying a rule's triggers, you can add actions that the application performs when trigger conditions are met.

Specifying an E-mail Action

You can configure the application to send an e-mail message when the specified trigger is fired.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

---

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **E-mail** from the **Actions** list at the bottom left side of the dialog box. The **E-mail** information displays, as shown in Figure 73.

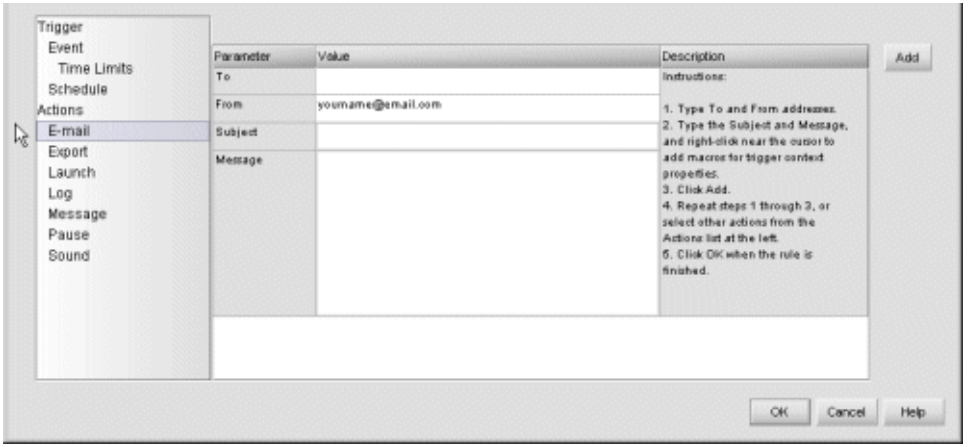


Figure 73: Add Rule dialog box (E-mail)

4. Enter the recipients' e-mail addresses, separating multiple addresses with semi colons in the **To** parameter's value.
5. Enter your e-mail address in the **From** parameter's value.
6. Enter a subject for the e-mail in the **Subject** parameter's value.
7. To insert a macro for values from the trigger's content, perform the following:
   a. Click in the **Value** column.
   b. Right-click and choose an argument from the menu.
8. Enter the body of your e-mail message in the **Message** parameter's value.
9. To insert a macro for values from the trigger's content, perform the following:
   a. Click in the **Value** column.
   b. Right-click and choose an argument from the menu.
10. Click **Add**.

Specifying an Export Action

You can configure the Event Management feature to export data when the specified trigger is fired.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **Export** from the **Actions** list at the bottom left side of the dialog box. The **Export** information displays, as shown in Figure 74.

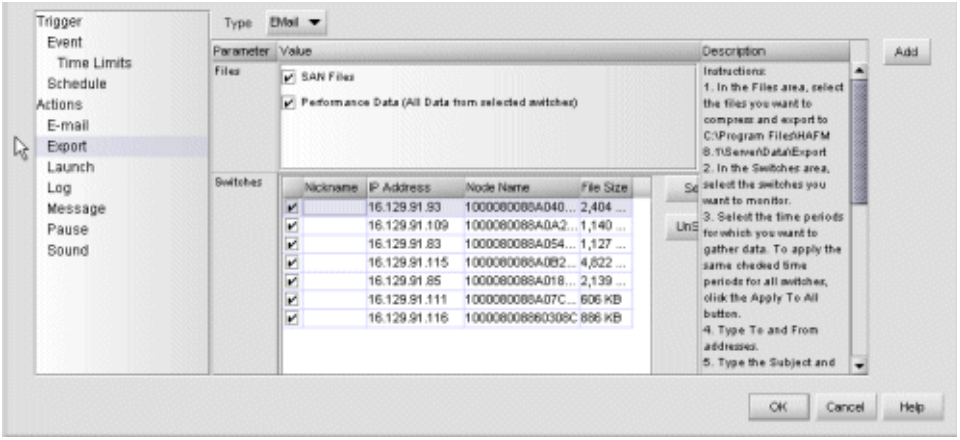


Figure 74: Add Rule dialog box (Export)

4. Choose the destination for the export from the **Type** drop-down list.
5. Choose the types of information you want to export from the **Files** area. The options may differ depending on the export destination.

Note: If you are not exporting performance data, skip step 6.

6. Choose the switches for which you want to export performance data from the **Switches** area.
7. Click **Add**.

Specifying a Launch Action

You can configure the Event Management feature to launch an application when the specified trigger is fired.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

Note: Before configuring the Event Management feature to launch a script, verify that the script launches the application successfully on the appliance.

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **Launch** from the **Actions** list at the bottom left side of the dialog box. The **Launch** information displays, as shown in Figure 75.

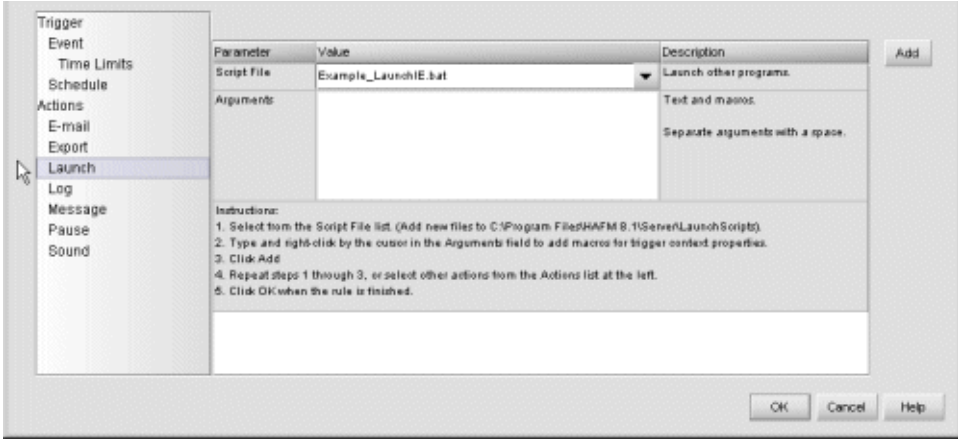


Figure 75: Add Rule dialog box (Launch)

4. Choose an option from the **Script File** parameter's value. You can add script files to this list by copying them to `<Install_Home>\Server\LaunchScripts\`.
5. Enter a script argument in the **Arguments** parameter's value.

6. To insert a macro for values from the trigger's content, perform the following:
   a. Click in the **Value** column.
   b. Right-click and choose an argument from the menu.
7. Click **Add**.

Specifying a Log Action

You can configure an additional master log entry that includes a custom description.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

---

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **Log** from the **Actions** list at the bottom left side of the dialog box. The **Log** information displays, as shown in Figure 76.

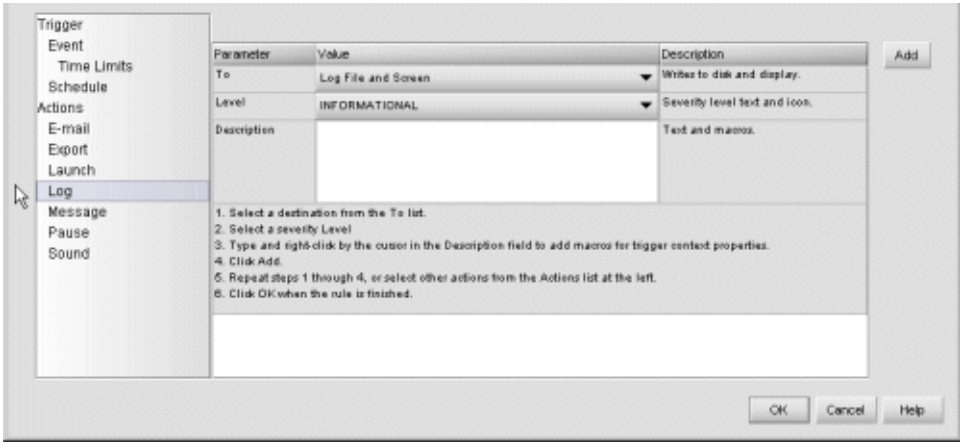


Figure 76: Add Rule dialog box (Log)

4. Choose an option from the **To** parameter's value.
5. Choose an option from the **Level** parameter's value.

6. Enter a description in the **Description** parameter's value.
7. To insert a macro for values from the trigger's content, perform the following:
   a. Click in the **Value** column.
   b. Right-click and choose an argument from the menu.
8. Click **Add**.

Specifying a Message Action

You can configure the application to display a pop-up message on all open clients when the specified trigger is fired. You can choose to display either informational, warning, or fatal icons in the message. The title bar displays the rule number, rule name, and "message." For example, "Rule 23 Switch Offline Message." The time and date are automatically inserted and multiple messages display in a single pop-up window.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

---

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **Message** from the **Actions** list at the bottom left side of the dialog box. The **Message** information displays, as shown in Figure 77.

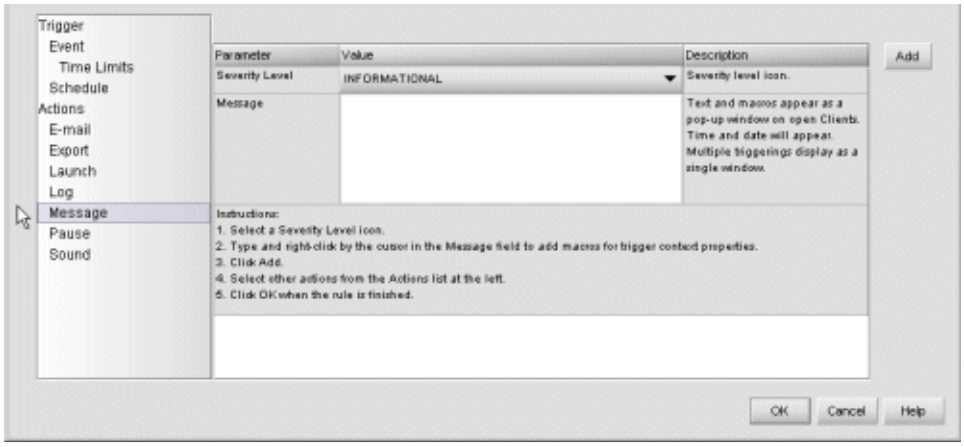


Figure 77: Add Rule dialog box (Message)

4. Choose an option from the **Severity Level** parameter's value.
5. Choose an option from the **Message** parameter's value.
6. To insert a macro for values from the trigger's content, perform the following:
   a. Click in the **Value** column.
   b. Right-click and choose an argument from the menu.
7. Click **Add**.

Specifying a Pause Action

You can configure the application to pause between actions when the specified trigger is fired.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

---

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **Pause** from the **Actions** list at the bottom left side of the dialog box. The **Pause** information displays, as shown in Figure 78.

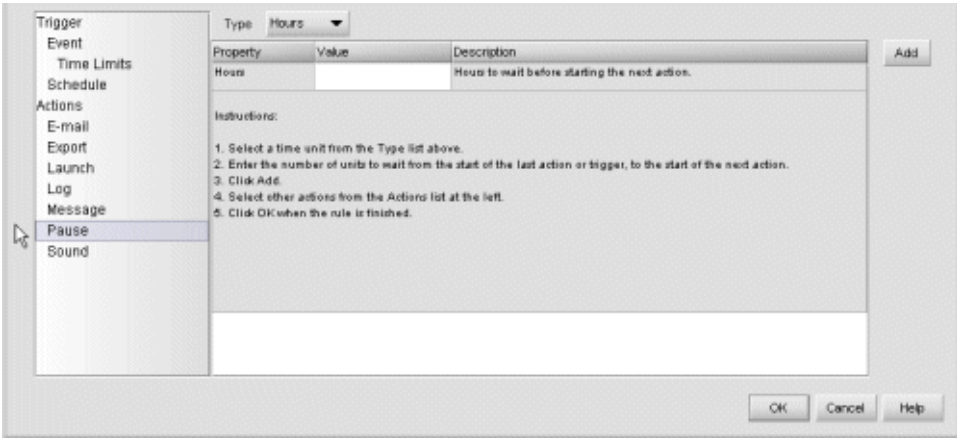


Figure 78: Add Rule dialog box (Pause)

4. Choose a time unit from the **Type** drop-down list.
5. Enter the number of units to wait in the **Value** field.
6. Click **Add**.

Specifying a Sound Action

You can configure the application to play a sound when the specified trigger is fired.

Note: Before specifying an action, you should specify the rule's triggers. See "About Triggers" on page 128 for instructions.

---

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **New**. The **Add Rule** dialog box displays, as shown in Figure 70 on page 134.
3. Choose **Sound** from the **Actions** list at the bottom left side of the dialog box. The **Sound** information displays, as shown in Figure 79.

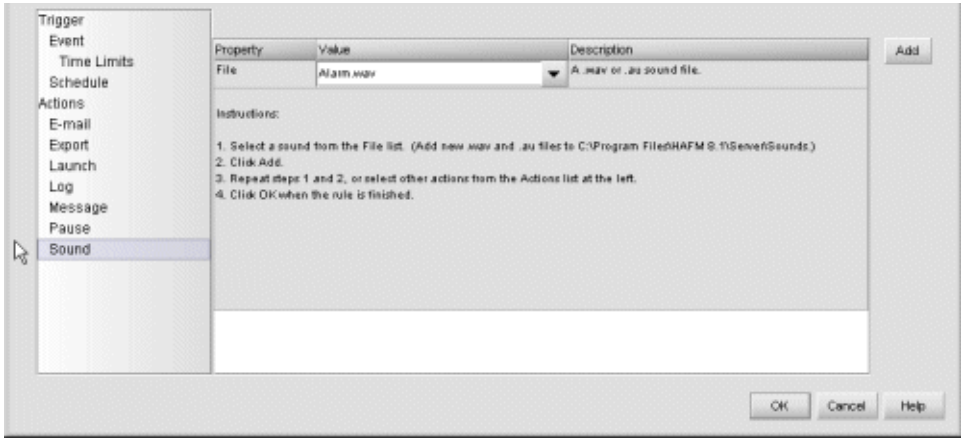


Figure 79: Add Rule dialog box (Sound)

4. Choose a sound from the **File** parameter's value. You can add sounds to this list by posting sound files to `<Install_Home>\Server\Sounds\`.
5. Click **Add**.

Editing a Rule

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Choose the rule you want to edit from the **Rules** table.
3. Click **Edit**. The **Edit Rule** dialog box displays.
4. Edit the rule as desired.
5. Click **OK**.

Copying a Rule

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Choose the rule you want to copy from the **Rules** table.
3. Click **Copy**. A copy of the selected rule is assigned a new rule number.

Deleting a Rule

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Choose the rule you want to delete from the **Rules** table.

Note: To select a non-contiguous set of rules, press CTRL and click each rule.

3. Click **Delete**. A confirmation message displays a list of the rules to be deleted.
4. Verify the list of rules and click **Yes**.

Activating Rules

Activating an Existing Rule

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Choose the rule you want to activate from the **Rules** table.

Note: To select a non-contiguous set of rules, press CTRL and click each rule.

3. Click **Activate**. A confirmation dialog box displays.
4. Click **Yes**. Each active rule displays a green flag in the **Active** column.

Activating a New Rule

1. Verify that the **Active** check box on the **Add Rule** or **Edit Rule** dialog box is selected.
2. Click **OK**. The rule is highlighted in the **Rules** table and displays a green flag in the **Active** column.

Deactivating Rules

Deactivating an Existing Rule

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Choose the rule you want to deactivate from the **Rules** table.

Note: To select a non-contiguous set of rules, press CTRL and click each rule.

Note: All active rules are marked with green flags.

---

3. Click **Deactivate**. A confirmation dialog box displays.
4. Click **Yes**. The green flag disappears from the **Active** column.

Deactivating a New Rule

1. Verify that the **Active** check box on the **Add Rule** or **Edit Rule** dialog box is not selected.
2. Click **OK**. The **Active** column does *NOT* display a green flag.

Turning the Event Management Feature On or Off

1. Click the **Event Management** tab on the main window. The Event Management tab displays, as shown in Figure 69 on page 133.
2. Click **On** or **Off** in the top right corner of the page.

FICON Management Server

The FICON Management Server is a keyed feature that allows host control and inband management of the director or switch through an IBM System/390 or zSeries 900 Parallel Enterprise Server server attached to a director or switch port. The server communicates with the switch or director through a FICON channel. Control of connectivity and statistical product monitoring are provided through a host-attached console.

Installation

To install and enable this option, choose the **Configure Feature Key** option on the Element Manager **Configure** menu.

Configuring the FICON Management Server

Use this procedure to configure whether the host is the controlling manager.

The optional FICON Management Server feature must be installed in order to perform this procedure.

- **Enable Management Server**—Click this check box to add a check mark and enable the management server. Click the check mark to remove it and disable this feature.
- **Switch Clock Alert Mode**—Click this check box to display a check mark and enable clock alert mode. If this is enabled, the following occurs when users set the date and time through the Configure Date and Time dialog box (**Configure** menu):
  - If you enable **Periodic Date/Time Synchronization**, an error message displays indicating that Clock Alert Mode must be cleared to enable automatic synchronization of the date and time.
  - If you manually set the date and time (**Periodic Date/Time Synchronization** is not enabled), a confirmation dialog box displays. You must click **OK** on that dialog box to continue manual configuration.
- **Host Control Prohibited**—Click this check box to display a check mark and prohibit a host management program from changing configuration and connectivity parameters on the switch. In this case, the host program has read authorization only and cannot make changes. When the check mark is not displayed, a host program can change configuration and connectivity parameters on the switch.

- **Programmed offline state control**—Click this check box to display a check mark and enable a host management program to control the switch's offline and online state. When a check mark is not displayed, a host program cannot set the switch online or offline.
- **Active=Saved**—Click this check box to display a check mark and enable the **active=saved** function for the IPL address configuration.
  - If **Active=Saved** is enabled (check mark), the IPL and the active address configuration are maintained as identical configurations. If a new configuration is activated through the **Configure Addresses - "Active"** dialog box, that configuration becomes the IPL address configuration.
  - If **Active=Saved** is not enabled (no check mark), the IPL address configuration and the active configuration are not maintained as identical, and may be different configurations. If the feature *is not* enabled, you can modify the IPL configuration through the **Configure Addresses - "Active"** dialog box. If the feature *is* enabled, the IPL file is locked to modification through the **Configure Addresses - "Active"** dialog box.
- **Code Page**—Consider the language required for the port name display that displays on the HAFM appliance. Language support is provided through character set 697 for all Extended Binary-Coded Decimal Interchange Code (EBCDIC) pages.

  When planning the installation, select the EBCDIC code page for displaying host-assigned port names or the CUP name. As an example, if the code page for Italy is selected and a port name is assigned in Italian by the host management program, then the Italian language port name displays in the Element Manager.

  This field lists the code pages that are available for configuration. The default code page is United States/Canada 00037. See the following table for other code pages:

Table 8: Port Name Language Code Pages

Code Page Name	Code Page	Hexadecimal CPGID
United States/Canada	00037	0025
Germany/Austria	00273	0111
Brazil	00275	0113
Italy	00280	0118
Japan	00281	0119
Spain/Latin America	00284	011C

Table 8: Port Name Language Code Pages (Continued)

Code Page Name	Code Page	Hexadecimal CPGID
United Kingdom	00285	011D
France	00297	0129
International #5	00500	01F4

Configuration Procedure

To configure the FICON management server, use the following steps:

1. Choose **Configure > Management Server** from the Element Manager window. The Configure FICON Management Server dialog box displays, as shown in Figure 80.

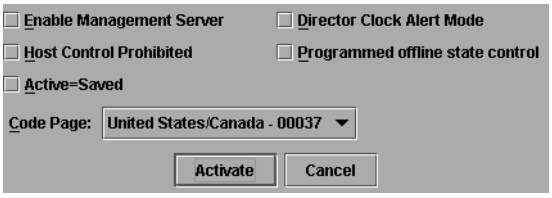


Figure 80: Configure FICON Management Server dialog box

2. Enable or disable the management server by clicking **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)
3. Enable or disable switch clock alert mode by clicking the **Director Clock Alert Mode** check box. When a check mark displays, the alert mode is enabled.
4. Allow or prohibit host control by clicking the check box in the **Host Control Prohibited** field. When a check mark displays, host control is prohibited.
5. Allow or prohibit offline state control by clicking the check box in the **Programmed offline state control** field. When a check mark displays, programmed control of the offline state is allowed.
6. Enable or disable Active=Saved mode by clicking the check box in the **Active=Saved** field. When a check mark displays, the Active=Saved mode is enabled.
7. If necessary, choose a code page from the **Code Page** drop-down list.
8. Activate changes and close the dialog box by clicking the **Activate** button.

9. If you are finished configuring the switch, back up the configuration data.

Open Systems Management Server

The Open System Management Server (OSMS) is a keyed feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device. This device is attached to a director or switch port. The device communicates with the switch or director through Fibre Channel common transport (FC-CT) protocol.

Installing the Open Systems management Server

To install and enable this option, perform the following:

1. Obtain the feature key. For more information, see “Managing Users” on page 57.
2. Choose **Configure > Features** from the Element Manager window. The Configure Feature Key dialog box displays, as shown in figure Figure 81.

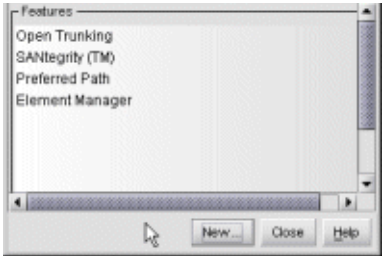


Figure 81: Configure Feature Key dialog box

3. Click New. The New Feature Key dialog box displays, as shown in .

Figure 82: New Feature Key dialog box

4. Enter the feature key in the Key field.
5. Click **OK**.

Configuring the Open Systems Management Server

Use these procedures to configure the open systems inband management program to function with the switch.

The optional Open Systems Management Server feature must be installed in order to perform this procedure.

To configure the Open Systems Management Server, use the following steps:

1. Choose **Configure > Management Server** from the Element Manager window. The Configure Open Systems Management Server dialog box displays, as shown in Figure 83.

Figure 83: Configure Open Systems Management Server dialog box

2. Enable the management server by clicking the **Enable Management Server** check box. (To disable the management server, click the check box again to remove the check mark.)
3. Click the check box in the **Host Control Prohibited** field to display a check mark and to prohibit the host management program from changing configuration and connectivity parameters on the switch. In this case, the host program has read-only access to configuration and connectivity parameters. Clicking the check box when it contains a check mark removes the check mark and allows a host program to change configuration and connectivity parameters on the switch.
4. To activate changes and close the dialog box, click **Activate**.
5. If you are finished configuring the switch, you can back up the configuration data.

SANtegrity Features

SANtegrity includes a set of features that enhance security in Storage Area Networks (SANs) that contain a large and mixed group of fabrics and attached devices. Through these features you can allow or prohibit switch attachment to fabrics and device attachment to switches. These features are enabled by purchasing a feature key, then enabling the key through the Configure Feature Key dialog box.

SANtegrity Binding features include:

- Fabric Binding
- Switch Binding

Enterprise Fabric Mode—Although this is not a keyed feature, the SANtegrity Fabric Binding and Switch Binding must be installed before you can use the Enterprise Fabric Mode function through the **HAFM Fabrics** menu.

Fabric Binding

This feature is managed through the **Fabric Binding** option, available through the **Fabrics** menu in HAFM when the **Fabrics** tab is selected. Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Enable/Disable and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by World Wide Name (WWN) and domain ID, the **Insistent Domain ID** option in the Configure Switch Parameters dialog box is automatically enabled if Fabric Binding is enabled.
- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director or switch is offline, you can disable Insistent Domain ID, but this disables Fabric Binding.

- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

Switch Binding

This feature is managed through the **Switch Binding** submenu options available on the Element Manager **Configure** menu. Using **Switch Binding**, you can specify devices and switches that can attach to director and switch ports. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a switch or director.

Configuring Switch Binding Overview

To configure Switch Binding, you must first activate the feature using the Switch Binding – State Change dialog box while selecting the type of port where you want to restrict connection (connection policy). Possible selections are E_Ports, F_Ports, or all types.

If the director or switch is online, activating Switch Binding populates the Membership List in the Switch Binding - Membership List dialog box (Element Manager) with the following WWNs currently connected to the director or switch, depending on the connection policy set in the Switch Binding – State Change dialog box:

- WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.
- WWNs of switches connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached switch.
- WWNs of devices connected to F_Ports and switches connected to E_Ports (all-ports connection policy).

Notes

- When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, switches, or both that are currently connected to the switch.
- If the switch is offline and you activate Switch Binding, the Membership List is not automatically populated.
- Edits to the Switch Binding Membership list is maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and switches from connecting with director or switch ports by removing them from the Membership List in the Switch Binding – Membership List dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and switches.

Enable/Disable Switch Binding

Use the following procedure to enable and disable switch binding:

1. Choose **Configure > Switch Binding > Change State** from the Element Manager window. The Switch Binding – State Change dialog box displays (Figure 84).

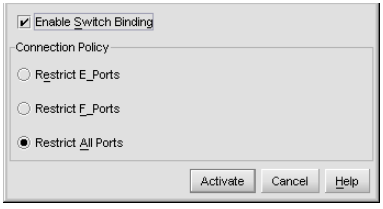


Figure 84: Switch Binding State Change dialog box

2. Perform one of the following steps:
   - To disable Switch Binding (a check mark displays in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to remove the check mark, then click **Activate**.
   - To enable Switch Binding (check mark is not in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to add a check mark. Go on to step 3 to set the Connection Policy.
3. Click one of the **Connection Policy** options:
   - **Restrict E_Ports**—Select if you want to restrict connections from specific switches to switch E_Ports. Switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.
   - **Restrict F_Ports**—Select if you want to restrict connections from specific devices to switch F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Switches are allowed to connect to any E_Port.

- **Restrict All**—Select if you want to restrict connections from specific devices to switch F_Ports and switches to switch E_Ports. Device and switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection.

4. Click **Activate** to enable the changes and close the dialog box.
5. Edit the Switch Membership List through the Switch Binding – Membership List dialog box to add or remove switches and devices that are allowed to connect with the switch.

Editing the Switch Membership List

1. Choose **Configure > Switch Binding > Edit Membership List** from the Element Manager window. The Switch Binding – Membership List dialog box displays (Figure 85).

   The WWNs of devices and switches that can currently connect to switch ports are listed in the **Switch Membership List** panel.

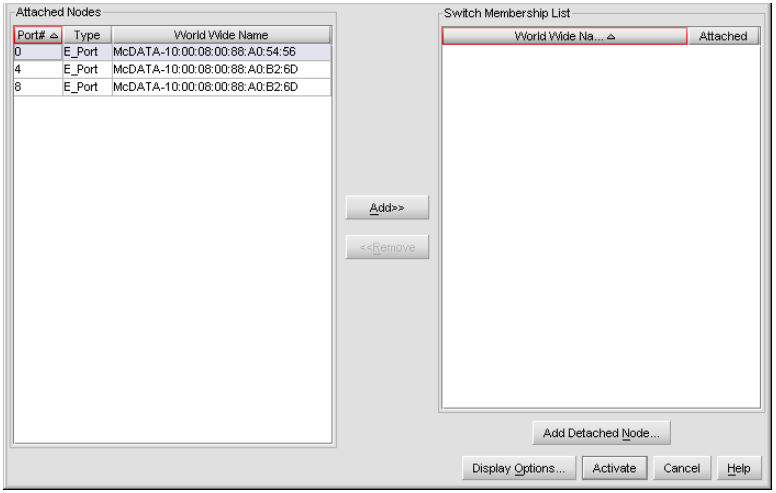


Figure 85: Switch Binding Membership List dialog box

See "Configuring Switch Binding Overview" on page 155 for information on how the Switch Membership List is populated with WWNs according to options set in the Switch Binding – State Change dialog box.

2. If nicknames are configured for WWNs through HAFM and you want these to display instead of WWNs in this dialog box, click **Display Options**. The Display Options dialog box displays.
3. Click **Nickname**, then click **OK**.
4. To prohibit connection to a switch port from a WWN currently in the Membership List, click the WWN or nickname in the **Membership List**, then click **Remove**. The WWN or nickname moves to the **Node List** panel. WWNs can only be removed from the fabric if any of the following is true:
   - The switch is offline.
   - Switch Binding is disabled.
   - The switch or device with the WWN is not connected to the switch.
   - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding – State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to Restrict F_Ports.
   - The switch or device with the WWN is connected to a port that is blocked.
5. The switch or device with the WWN is not currently connected to the switch (detached node).
6. WWNs can be added to the **Switch Membership List** (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a switch port from a WWN in the **Attached Nodes** panel, select the WWN or nickname in the **Attached Nodes** panel, then click the **Add** button. The WWN or nickname moves to the **Switch Membership List** panel.
7. To add a WWN for a device or switch not currently connected to the switch, click **Add Detached Node**. The Add Detached Node dialog box displays.
8. Enter the appropriate WWN or nickname (if configured through HAFM) and click **OK**. The WWN or nickname displays in the **Switch Membership List**.
9. Click **Activate** to enable the changes and close the dialog box.

Enable/Disable and Online State Functions

In order for Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Switch Binding can be enabled or disabled whether the switch is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.
- If Enterprise Fabric Mode is enabled and the director or switch is offline, you can disable Switch Binding which will also cause Enterprise Fabric Mode to be disabled.
- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.
- WWNs can only be removed from the Switch Membership List if any of the following are true:
  - The director or switch is offline.
  - Switch Binding is disabled.
  - The switch or device with the WWN is not connected to the director or switch.
  - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding – State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to Restrict F_Ports.
  - The switch or device with the WWN is connected to a port that is blocked.
  - The switch or device with the WWN is not currently connected to the director or switch (detached node).
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the Switch Membership List.

Zoning with Switch Binding Enabled

Note that SANtegrity has no effect on existing zoning configurations. However, note that if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the device cannot log in to the director or switch port and cannot connect to other devices in the zone with Switch Binding enabled.

Enterprise Fabric Mode

Enterprise Fabric Mode is an option available on the **Fabrics** menu in the *HAFM* application if the SANtegrity feature key is installed. This option automatically enables the following features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. Note that there are specific requirements for disabling these parameters and features when the director or switch is offline or online.

Fabric Binding

This is a SANtegrity feature enabled through the **Fabrics** menu in HAFM that allows or prohibits switches and directors from merging with a selected fabric. See "Enable/Disable and Online State Functions" on page 154 for details on enabling/disabling Fabric Binding with Enterprise Fabric Mode.

Switch Binding

This is a SANtegrity feature enabled through the **Configure** menu in the Element Manager that allows or prohibits switches and/or directors from connecting to switch E_Ports or F_Ports. See "Enable/Disable and Online State Functions" on page 154 for details on enabling/disabling Switch Binding with Enterprise Fabric Mode enabled.

Rerouting Delay

Rerouting Delay is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the Element Manager application. Rerouting Delay ensures that frames are delivered through the fabric in order to their destination.

If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if the path's hop count is less than a previous path with a minimum hop count. This rerouting may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path. If Rerouting Delay is enabled, traffic ceases in the fabric for the time specified in the **E_D_TOV** field of the Configure Fabric Parameters dialog box (**Configure** menu). This delay enables frames sent on the old path to exit to their destination before new frames begin traversing the new path.

If Enterprise Fabric Mode is enabled, the **Rerouting Delay** option is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Rerouting Delay also disables Enterprise Fabric Mode.

Domain RSCNs

This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the *Element Manager* application. Domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBAs) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

If Enterprise Fabric Mode is enabled, this parameter is automatically enabled and cannot be disabled unless the director or switch is offline. In this case, disabling Domain RSCNs also disables Enterprise Fabric Mode.

Insistent Domain Identification (ID)

This is a parameter in the Configure Switch Parameters dialog box, available from the **Configure** menu in the *Element Manager* application. Enabling this option sets the domain ID configured in the **Preferred Domain ID** field in the Configure Switch Parameters dialog box as the active domain identification when the fabric initializes. A static and unique domain identification is required by the Fabric Binding feature because the feature's Fabric Membership list identifies switches by WWN and Domain ID. If a duplicate preferred domain ID is used, and insisted, warnings occur when directors and switches are added to a Fabric Membership List.

If Fabric Binding or Enterprise Fabric Mode is enabled, this option is automatically enabled and cannot be disabled unless these options are disabled when the director or switch is offline. If the director or switch is online, disabling Insistent Domain ID disables Enterprise Fabric Mode and Fabric Binding.

Open Trunking

Interswitch links (ISLs) connect ports between E_Ports on Fibre Channel switches and link these switches into a multiswitch fabric. Multiple ISLs may be connected between the switches in the fabric. Data from an attached end device (server or storage) flows through these ISLs to a target end-device connected to a switch somewhere in the fabric. A data flow is data received from a specified receive port that is destined for a port in a specified target domain (switch). The list of ISLs that are candidates for being rerouted (to or from) is derived from the fibre shortest path first (FSPF) algorithm.

The Open Trunking feature monitors the average data rates of all traffic flows on ISLs (from a receive port to a target domain) and periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimize bandwidth use. The objective of Open Trunking is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

Load-balancing among the ISLs does not require user configuration, other than enabling Open Trunking. However, you can modify or "tweak" default settings for congestion thresholds (per port) and low BB_credit threshold if desired.

In particular, you do not need to manually configure ISLs into "trunk groups" of redundant links where data can be "off-loaded." Candidate links for rerouting flow are identified and maintained automatically. This means that flow may be rerouted onto a link that goes to a different adjacent switch as long as that link is on the least cost/shortest path to the destination domain ID.

To install and enable this option, select the **Configure Feature Key** option under the Element Manager's **Configure** menu.

Enabling and Configuring Open Trunking

To enable Open Trunking for a specific switch and configure threshold values and event notification options, use the following steps.

1. Choose **Configure > Open Trunking**. The Configure Open Trunking dialog box displays, as shown in Figure 86.

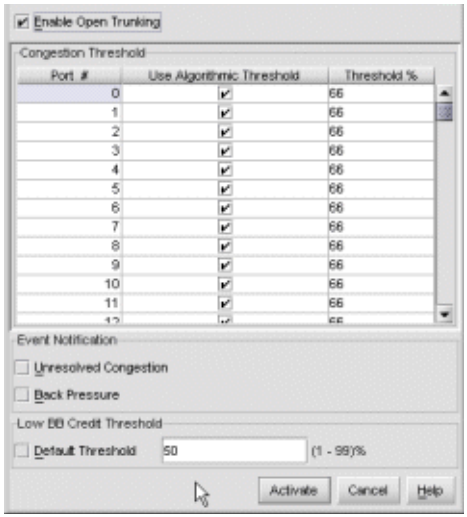


Figure 86: Configure Open Trunking dialog box

2. Enable Open Trunking by clicking the **Enable Open Trunking** check box to display a check mark.
3. Set the C**ongestion Thresholds** for ports as percentages of link bandwidths, in the range of 1% through 99%. These thresholds are used only when a port becomes an ISL. When the link's traffic load becomes greater than this percentage, the link is seen as "congested" and traffic is rerouted (if possible) to an uncongested link. Note that rerouting may not be possible if there are no alternate links available or if alternate links are congested or have no available BB_Credit.

Note: Using default settings for port congestion thresholds should work well in most cases. This step is not required.

Set the **Congestion Threshold** using one of these methods:

- Click the check box under the **Use Algorithmic Threshold** column to display a value under the **Threshold %** column. This value is computed by the feature's rerouting algorithm. If you click this check box, you cannot enter a value into the **Threshold %** column for the port.
- If you click the check box to remove the check mark, any value that was set in the **Threshold %** column for the port redisplays.

- Click in the **Threshold %** column and enter a value in the range of 1 through 99.

Note: If no threshold is entered for a port, a default value is used that is based on port type (1 Gb/s or 2 Gb/s) and channel bandwidth. This field cannot be left blank.

---

4. Set **Event Notification** options. Note that, if enabled, these notifications occur the first time the events occur. Notifications are not resent while the problem persists.
   - **Unresolved Congestion**—Click this check box to display a check mark and enable notification. If enabled, an "unresolved congestion" entry is made to the Event Log and an SNMP trap are generated if trap recipients are configured through the Configure SNMP dialog box.

     An unresolved congestion event occurs when the rerouting algorithm cannot find a path for rerouting data flow and relieving congestion on an ISL.
   - **Back Pressure**—Click this check box to display a check mark and enable this option. If enabled, a back pressure entry is made to the **Event Log** and an SNMP trap are generated if trap recipients are configured through the Configure SNMP dialog box.

     A back pressure event occurs when the percentage of time the ISL has no available BB_Credit exceeds the low BB_credit threshold. A separate event also occurs when the back pressure condition ends.
5. Set the **Low BB_Credit Threshold**.

Note: Using default settings for low BB_Credit threshold should work well in most cases. This step is not required.

The threshold value is the percentage of time that the transmitting link has no BB_Credit. This value is also used when determining routes for a transmit link. An ISL that has no BB_Credit for longer than this time percentage cannot be the recipient of traffic rerouted from other ISLs. Traffic on this ISL may be rerouted by Open Trunking even if the ISL is not congested.

Two options are available:

- Click **Default Threshold** and a default value (1 to 99%) appears in the **threshold** field. If the default is enabled, you cannot enter values into the field.
- Click in the **threshold** field and enter a value from 1 to 99.

6. Click **Activate** to enable these values on the switch and close the dialog box.

Using the Pop-Up Menu

Right click on columns in the **Configuration Threshold** table to display menu options that globally change values in the column cells.

- **Use Algorithmic Threshold**—Right click in the column to display these options:
  - **Set all to Default**—Adds check marks to all check boxes in this column and sets all cells of **Threshold %** column to default values.
  - **Clear All**—Clears all check boxes in this column and restores values in cells of **Threshold %** column with previous values.
- **Threshold %**—Right click in the column to display these options:
  - **Set All To xx**—Sets all cells in this column to the value (xx) that you clicked.
  - **Restore All**—Sets all cells in the column to the previous values.

Open Trunking Log

The Open Trunking log as shown in Figure 87, provides details on flow rerouting that is occurring through switch ports.

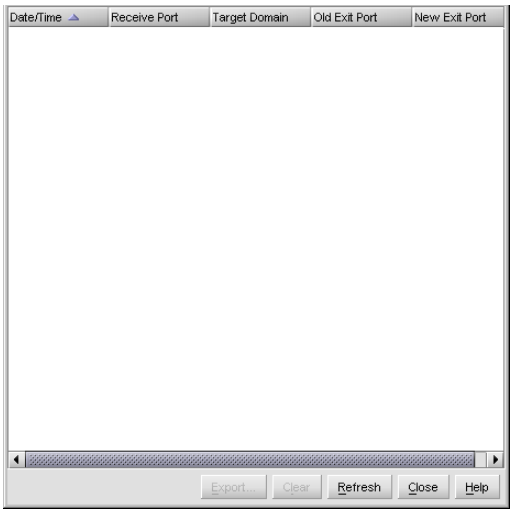


Figure 87: Open Trunking log

- **Date and Time**—Date and time that action occurred.
- **Receive Port**—The decimal receive port number on the local switch associated with the flow that was rerouted.
- **Target Domain**—The decimal domain ID associated with the flow that was rerouted.
- **Old Exit Port**—The decimal exit port number on this switch that the flow used to get to the target domain.
- **New Exit Port**—The decimal exit port number on this switch that the flow now uses to get to the target domain.

Monitoring Performance

This section provides instructions for monitoring SAN devices using the Performance Module. For information regarding event monitoring and notification, refer to the HAFM online Help which includes the following topics.

Monitoring Connection Utilization

The application displays the percentage of utilization on the trunks as well as on the utilization legend. To display the connection utilization legend, perform the following:

1. Choose **Monitor Utilization > On** (or **CTRL + U**). The Connection Utilization Legend displays, as shown in Figure 88.

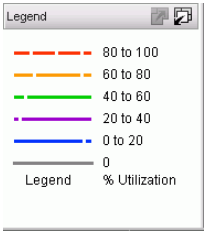


Figure 88: Utilization Legend

To turn utilization off, perform the following:

1. Choose **Monitor > Utilization > Off**.

In the utilization legend, the color and the length of the lines indicate the bandwidth utilization. Table 9 describes the Utilization legend.

Table 9: Utilization Legend Description

Line Color	Utilization
Red line	80% to 100% utilization
Orange line	60% to 80% utilization
Light green line	40% to 60% utilization
Dark purple line	20% to 40% utilization
Blue line	0% to 20% utilization
Gray line	0% utilization

Monitoring Switch Performance

You can monitor a switch's performance through a performance graph, which displays transmit, receive, and error data from the switch ports to the connected devices. The graphs can be sorted by the Errors, Transmit, and Receive data.

1. Right-click a switch icon and choose **Performance Graphs**. The Performance Graph displays, as shown in Figure 89.

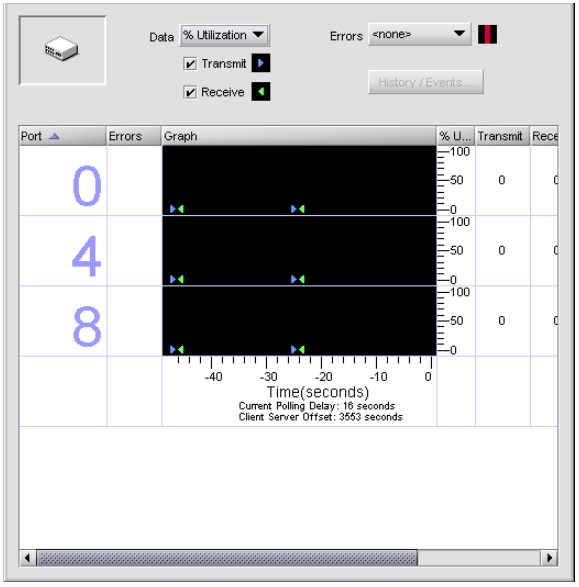


Figure 89: Switch Performance graph

2. Choose the type of data to display from the **Data** drop-down list.
3. Choose the error data to display from the **Errors** drop-down list.
4. Click the **X** button at the top of the window to close it.

Gathering and Viewing Performance Data

You can collect performance data about your SAN and then view it in a report or export it and distribute the data to others.

Storing Performance Data

You can specify whether you want the application to store performance information. To enable storing of performance data, perform the following:

1. Choose **Monitor > Performance > Store Data**.

Viewing Performance Data

You can generate HTML reports of performance data, which you can view through the application or through a Web browser. Refer to the HAFM online Help for more information.

Exporting Performance Data

You can export SAN performance data to communicate issues to the support center, capture network status, and archive historical data. You can export performance data to various outputs. For more information about exporting, refer to the HAFM online Help.

Note: Currently, you can only export to the same versions of the application.

---

1. Choose **SAN > Export**. The Export dialog box displays a list of file types that can be exported, along with their sizes, as shown in Figure 90.

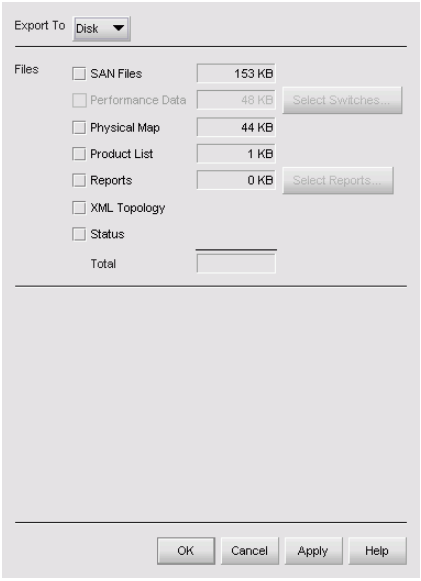


Figure 90: Export dialog box

2. Select one of the following options from the **Export To** drop-down list.

Note: Some file types may not be available based on the export destination you selected in the previous step.

- **Disk**—Saves the exported files to the disk in `<Install_Home>\Client\Data\`.
- **EMail**—Mails the exported files as an e-mail attachment directly from the application.

3. Choose **Performance Data**. Select other types of files to export, if desired.
4. If you want to export performance data for only specific switches, click **Select Switches** and select the switches for which you want to export performance data.
5. If you are exporting to **disk**, skip to step 6.
   or
   If you are exporting to **email**, enter information in the following fields:
   — **Mail To**—Enter the recipient's e-mail address.

— **Mail List**—Click to select from a list of e-mail addresses.

— **From**—Enter your e-mail address.

— **Subject**—Enter a subject for the e-mail message.

— **Message**—Enter content for the e-mail message.

6. Click **OK** to export the files and close the dialog box.
7. Click **OK** at the confirmation window.

Monitoring Port Performance

You can monitor the performance of individual switch ports in the SAN through a port performance graph. The Performance Graph displays the performance of the switch and the devices connected to it. It also displays information about transmit and receive performance.

1. Right-click a switch icon and choose **Performance Graphs**. The Performance Graph displays, as shown in Figure 89 on page 168.
2. Highlight a port row and click **History/Events** or double-click a port row. The Port Performance Graph displays, as shown in Figure 91.

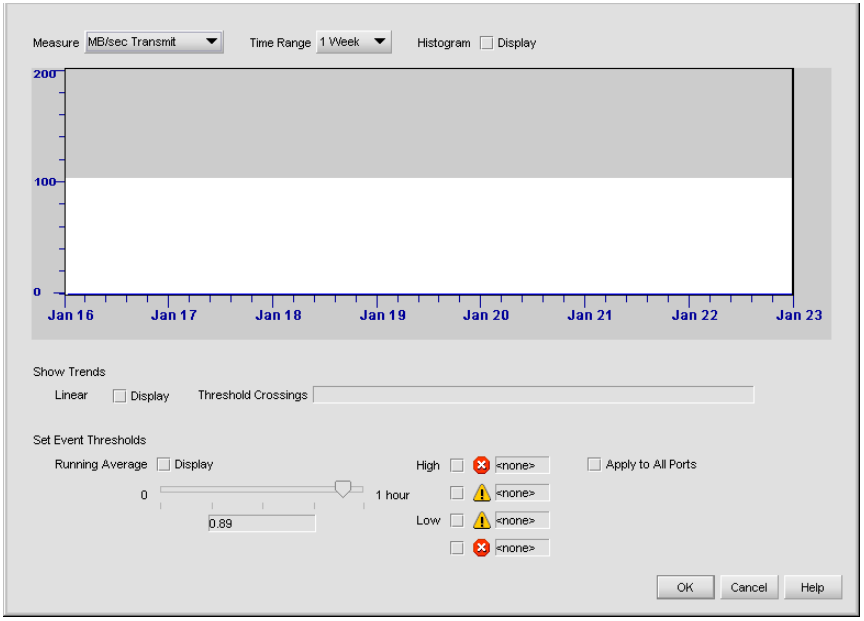


Figure 91: Port Performance Graph dialog box

3. Choose a different option from the **Measure** drop-down list to change the unit of measure for the graph.
4. Choose a different option from the **Time Range** drop-down list to change the time range for the graph.
5. Choose **Histogram Display** to display the percentage of utilization over a period of time.
   a. Move the **Histogram** slide-bar to the appropriate times to change the period of time. As you move the slide-bars, the display updates automatically.
6. Choose **Linear Display** to view a linear average of the trunk utilization.

   The application predicts potential threshold crossings. This function provides a forward-looking trend analysis and is intended to notify the user of resource modeling problems.
7. Choose **Running Average Display** to apply an averaging algorithm to the display.

   This display can be smoothed on a varying percentage of an hour. To change the display, move the slide-bar.
8. Choose the check boxes next to  and  icons to define the boundaries to configure both high and low usage performance warnings and critical thresholds.
9. Adjust the slide-bars at the right side of the display. As you move a slide-bar, the percentage of utilization displays in the field associated with the slide-bar that you are adjusting.
10. Set separate transmit and receive thresholds in either **%Utilization** or **MB/sec**. Set separate error thresholds. If **Running Average Display** is checked, your thresholds are only triggered if the running average crosses the threshold.
11. Click **Apply to All Ports** if you want to apply your changes to all ports on the device.
12. Click **OK**.

Setting Performance Thresholds

Through the application, you can configure both high and low usage performance warnings and critical thresholds.

Note: Discovery must be turned on to view threshold values.

1. Right-click a switch icon and choose **Performance Graphs**. The Performance Graph displays, as shown in Figure 89 on page 168.
2. Highlight a port row and click **History/Events** or double-click a port row. The Port Performance Graph displays, as shown in Figure 91 on page 171.
3. Choose the check boxes next to  and  icons to define the boundaries to configure both high and low usage performance warnings and critical thresholds.
4. Adjust the slide-bars at the right side of the display. As you move the slide-bar, the percentage of utilization displays in the field associated with the slide-bar that you are adjusting.
5. Click **Apply to All Ports** if you want to apply your changes to all ports on the device.
6. Click **OK**.

Note: Switch performance data and thresholds are indexed by their node name. This means if you move a switch from one location to another, it "brings" its performance data and thresholds with it. Additionally, if a threshold is set in one SAN file and the same switch is discovered in a different SAN file, the threshold is defined in both files.

Working with the Planning Module

This section provides instructions for using the optional Planning module to plan a SAN. The Planning module enables you to plan and evaluate a SAN before you implement the design. This can save considerable time and cost as you can evaluate the plan to find issues with the design. Another time-saving feature is that you can use a discovered SAN as the basis for a plan, eliminating the need to duplicate a design.

Planning Window

The planning window as shown in Figure 92, differs slightly from the window that displays a discovered SAN. In the planning window, there are three tabs—**Physical Map**, **Device List** and **Event Management**.

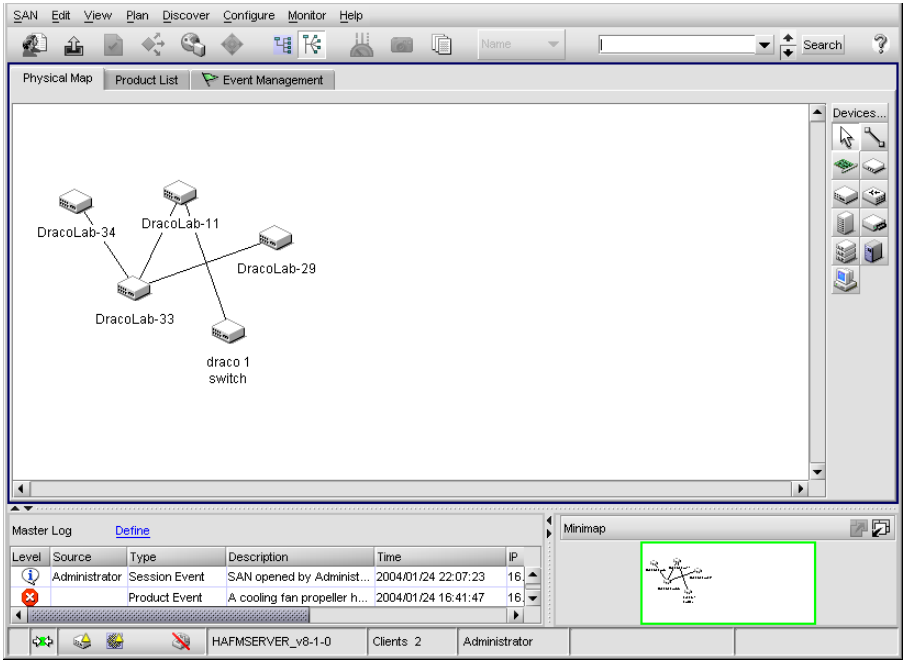
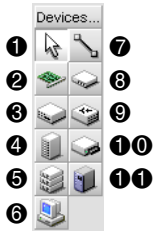


Figure 92: Planning window

Devices Toolbox

The **Devices** toolbox as shown in Figure 93, located on the right side of the planning window, provides tools to add, select, and connect devices in the planned SAN.



❶ Select Devices
❷ Insert HBA
❸ Insert Switch
❹ Insert Storage
❺ Insert JBOD
❻ Insert Server
❼ Connect Devices
❽ Insert Hub
❾ Insert Bridge
❿ Insert Tape Drive
⓫ Insert NAS

Figure 93: Devices Toolbox

Planning a New SAN

1. Choose **SAN > New Plan** (or **CTRL+N**). The New Plan dialog box displays, as shown in Figure 94.

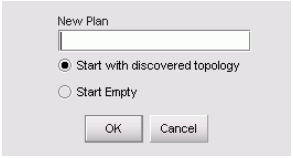


Figure 94: New Plan dialog box

2. Enter a name for the new plan in the **New Plan** field.
3. Click one of the following options:
   - Click **Start with discovered topology** to use the discovered topology as the basis for the new plan.
   - Click **Start Empty** to start the new plan with an empty topology.
4. Click **OK**.

Opening an Existing Plan

1. Choose **SAN > Open Plan** (or **CTRL+O**). The Open Plan dialog box displays, as shown in Figure 95.

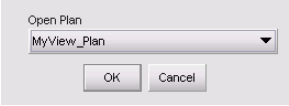


Figure 95: Open Plan dialog box

2. Choose a plan from the **Open Plan** drop-down list.
3. Click **OK**.

Designing a Plan

By designing a plan, you can configure, connect, and arrange planned devices before implementing the design. This enables you to envision and evaluate the plan.

Adding Planned Devices

You can either add devices one at a time or add multiple devices at the same time.

Adding Individual Devices

1. Click a device button on the **Devices** toolbox in the planning window.
2. Click on the Physical Map. The new planned device icon displays on the Physical Map.
3. Arrange planned icons as necessary.

Adding Multiple Devices

1. Click the **Devices** button on the **Devices** toolbox in the planning window. The Insert Multiple Devices dialog box displays, as shown in Figure 96.

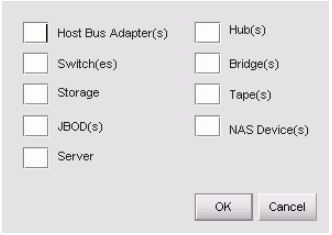


Figure 96: Insert Multiple Devices dialog box

2. Enter a quantity for each device type that you want to add.
3. Click **OK**.

Editing Port Types

You can edit a planned device's port types in the Planning window.

Note: This task can only be performed in Planning window.

---

1. Choose **View > Planned SAN**.
2. Add devices as desired. See "Adding Planned Devices" on page 176 for instructions.
3. Connect the devices using the **Connect Devices** icon () on the **Devices** toolbox.
4. Right-click a planned device icon and choose **Ports** to view the device's ports.
5. Click the black arrow next to the port number. The Port Properties dialog box displays, as shown in Figure 97.

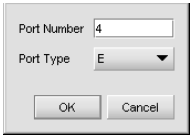


Figure 97: Port Properties dialog box

6. Enter the desired port number in the **Port Number** field.
7. Choose the desired port type from the **Port Type** drop-down list (only available for multi-port devices).

8. Click **OK**.
9. If desired, right-click the planned device icons and choose **Planned Device**. The device changes from a planned device to an implemented device.

Displaying a Planned Device as an Installed Device

Right-click on a planned device and choose **Planned Device** from the menu. If the **Planned Device** option is selected, the device icon displays inside a box icon. If the option is not selected, the device icon displays on its own.

Connecting Planned Devices

1. Connect the devices using the **Connect Devices** icon ( ) on the **Devices** toolbox.
2. Click a device on the Physical Map. A connection is created and associated with the first available port on the device.
3. Click another device on the Physical Map. The connection is associated with the first available port on the second device.

A connection displays between the two devices. If you want to make multiple connections, click the **Connect Devices** icon ( ), hold down the **Shift** key and click each device you want to connect. You can continue making connections as long as you hold down the **Shift** key.

Arranging Planned Devices

After adding devices to your plan, you can rearrange them as necessary.

1. Click the **Select Devices** icon ( ) on the **Devices** toolbox.
2. Click a planned device icon and drag it to the desired location.
3. Repeat as necessary.

Configuring Planned Devices

You can specify properties for planned devices just as you would for discovered devices.

1. Right-click a planned device icon and choose **Properties** from the menu. The planned device's Properties dialog box displays, as shown in Figure 98.

Figure 98: Planned device Properties dialog box

2. Type the nickname for the device in the **Nickname** field.
3. Enter or edit information as necessary.
4. Click **OK**.

Configuring Planned Ports

You can configure port numbers and types on planned devices.

Note: To configure planned ports, planned devices must be connected.

---

1. Right-click a planned device icon and choose **Ports** from the menu.
2. Click the small triangle next to the port number. The Port Properties dialog box displays, as shown in Figure 97 on page 177.
3. Edit the **Port Number** field.
4. Choose a port type from the **Port Type** drop-down list.
5. Click **OK**.

Deleting Planned Devices

To delete planned devices, perform the following:

1. Right-click on the planned device icon and choose **Delete** from the menu.

Evaluating a Plan Using Planning Rules

This section provides instructions for evaluating a plan using planning rules.

Planning Rules

Note: Planning rules should only be edited by advanced users.

Note: You must have Administrator privileges to set planning rules.

You can specify rules by which the application evaluates a plan. Rules are stored in the text file `<Install_Home>\Server\Config\Other\rules.dat`.

- **Planning Rules Syntax and Format**—Planning rules must follow a certain syntax and format. See Table 10 for descriptions of planning rule parameters.

```
set rule_id = SAN_1

where rule = "check_for_valid IPAddress for (device=switch or
device=hub or device=bridge)"

and description = "valid IP addresses must be specified for all
switches, hubs and bridges"

and headline = "Valid IP must be specified/property validation"

and errormssg = "The device labeled {0} has invalid IP address"

and remedy = "Please specify a valid IP address";
```

Table 10: Planning Rule Parameters

Parameter	Required	Description	Formatting
set rule_id	Yes	Sets the rule ID. The rule is no loaded if this is not specified.	Must be a unique value, but can be any length and any format.
where rule	Yes	Sets the actual rule. The rule is not loaded if this is not specified. See "Types of Rules—There are three types of rules that you can write to evaluate a plan:" on page 181 and "Keywords—When writing the where rule parameter, only certain keywords may be used." on page 183 for more information.	Use only the keywords provided; otherwise the rule fails.
description	No	Provides a more detailed description of the rule.	Must be prepended with an "And." Must be enclosed within quotation marks.
headline	No	Provides a short overview of the rule.	Must be prepended with an "And." Must be enclosed within quotation marks.
errormssg	No	Specifies the error message to display if the rule is violated during evaluation. If this statement is not specified, or if it is null, a generic error message displays.	Must be prepended with an "And." Must be enclosed within quotation marks.
remedy	No	Specifies a remedy for the rule violation. This text displays on the evaluation screen.	Must be prepended with an "And." Must be enclosed within quotation marks.

- **Types of Rules**—There are three types of rules that you can write to evaluate a plan:

— **Connection Rules**—Connection rules specify which devices can be connected in a plan.

Table 11: Connection Rules Syntax

Syntax	Description
do_not_connect (device=x)	Never connect device *x* to device *x*.
do_not_connect (device=x) to (device=y)	Never connect device *x* to *y*.
do_not_connect (device=x) to (device=y) through (device=z)	Never connect device *x* to *y* through *z*.
do_not_attach (device=x) to (device=y)	Never connect device *x* into a SAN which has device *y*.
connect (device=x)	Always connect device *x* to device *x*.
connect (device=x) to (device=y)	Always connect device *x* to *y*.
connect (device=x) to (device=y) through (device=z)	Never connect device *x* to *y* through *z*.

— **Property Validation Rules**—Property validation rules verify the validity or uniqueness of device names in a plan.

Table 12: Property Validation Rules Syntax

Syntax	Description
check_for_valid 'PropertyName' for (device=x)	Device *x* must have valid '*PropertyName*'.
'PropertyName' *should_be_unique_in* 'Types'	Cannot have duplicate '*PropertyName*' in the same '*Types*'.

— **Capacity Control Rules**—Capacity control rules verify the connections in a plan.

Table 13: Capacity Control Rules Syntax

Syntax	Description
total_connections (device = x) 'Operator' 2	The sum of connections to device *x* should be '*Operator*' than 2total_connections.
(device = x) 'Operator' MAXPORTS	The sum of connections to device *x* should be '*Operator*' than MAXPORTS.
total_connections (device = x) to (device = y) 'Operator' 2	The sum of connections from device *x* to device *y* should be '*Operator*' than 2.

- Keywords—When writing the `where rule` parameter, only certain keywords may be used.

Note: Keywords are not case sensitive.

  - **Types**
    - **Device**
    - **Network**
    - **Zone**
    - **Fabric**
    - **Switch**, **Hub**, **Bridge**, **NAS**, **HBA**, **Storage**, **Tape**, **JBOD**, **Loop**, **Server**—various types of devices
  - Property Names
    - **Wwn**—Node worldwide name
    - **Portwwn**—Port worldwide name
    - **model**—Device model
    - **IPAddress**—Device IP address
    - **serialNumber**—Device serial number
    - **vendor**—Device vendor
    - **Firmware**—Firmware on the device
    - **PortType**—Port type on a device

- **PortNumber**—Port number on a device
- **ZoneName**—Zone name
- **F_Port, FL_Port, TL_Port, E_Port, NL_Port, N_Port, H_Port, UNKNOWN_PORT**—Various types of ports
- **MAXPORTS**—Max ports for a device

— Operator Types

- **=**
- **<**
- **<=**
- **>**
- **>=**

Setting Planning Rules

Note: You must have Administrator privileges to set planning rules.

Use planning rules to specify criteria for a plan evaluation. Rules are stored in the text file `<Install_Home>\Server\Config\Other\rules.dat` and can only be edited or added through this file. You can open the *rules.dat* file using any text editor. Be sure to follow appropriate rule syntax when editing the file. See "Planning Rules Syntax and Format—Planning rules must follow a certain syntax and format. See Table 10 for descriptions of planning rule parameters." on page 180 for syntax information.

1. Choose **View > Planned SAN**. The Planning window displays.
2. Choose **Plan > Set Rules**. The Planning Rules dialog box displays, as shown in Figure 99.

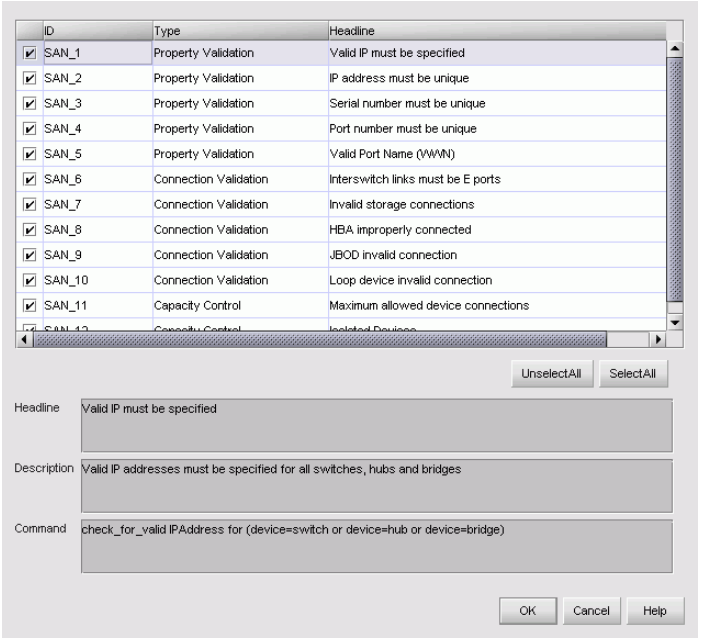


Figure 99: Planning Rules dialog box

3. Edit and write new rules by opening the `<Install_Home>\Server\Config\Other\rules.dat` file in a text editor.

Note: If spelling or syntax errors are detected, the rule may not display in the Planning Rules dialog box.

---

4. Choose the check boxes to select the rules you want to apply when evaluating the plan in the Planning Rules dialog box.
5. Click **OK**.

See "Evaluating a Plan" on page 185 for instructions on evaluating the plan using the rules you selected.

Evaluating a Plan

1. Open a plan to evaluate. See "Opening an Existing Plan" on page 176 for instructions.

2. Choose **Plan > Evaluate**. The application evaluates the plan and lists issues in the SAN Evaluation Report window.
3. Review the report. Click the hyperlinks to jump to devices and refer to the tips to determine resolutions.
4. Resolve the issues.
5. Choose **Plan > Evaluate** to re-evaluate the plan.
6. If more problems are identified, repeat step 2 - step 5.

Outputting a Plan

This section provides instructions for saving or exporting a plan.

Saving a Plan

After you have designed a plan, you can save it for future reference.

Saving the Plan with its Current Name

1. Choose **SAN > Save Plan**.
2. The plan is saved with the current name.

Saving the Plan with a New Name

1. Choose **SAN > Save as Plan**. The Save As dialog box displays.
2. Enter a new file name in the **Save As** field.
3. Click **OK**.

Exporting a Plan

You can export planning files to various outputs. Use this function to share a plan with others or to archive a plan for future reference.

1. Choose **SAN > Export**. The Export dialog box displays, as shown in Figure 100.

   The Export dialog box displays a list of file types that can be exported, along with their sizes.

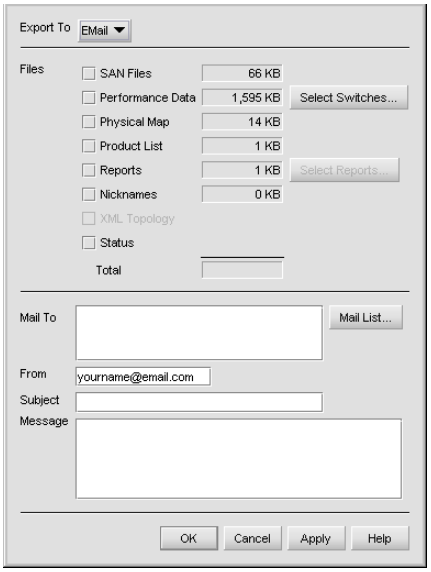


Figure 100: Export dialog box

2. Choose one of the following options from the **Export To** drop-down list:
   - **Disk**—Saves exported files to `<Install_Home>\Client\Data\<sanyymmddhhmmss>`.
   - **EMail**—Mails the exported files as an e-mail attachment directly from the application.
3. Choose the types of files you want to export.

Note: Some file types may not be available based on the export destination you selected in the previous step.

   - **SAN Files**—Exports the SAN files.
   - **Physical Map**—Exports the Physical Map, or topology.
   - **Product List**—Exports the Product List in tab-delimited format. To view the product list in table format, open it in Microsoft Excel.
   - **Reports**—Exports SAN reports.
   - **Nicknames**—Exports product nicknames.

- — **XML Topology**—Exports description of all fabric topologies in XML format.
- — **Status**—Exports SAN status data used by technical support.

4. If you are exporting to **Disk**, skip to step 6. Otherwise, continue to step 5.
5. If you are exporting to **EMail**, enter information in the following fields:
   - — **Mail To**—Enter the recipient's e-mail address.
   - — **Mail List**—Click to select from a list of e-mail addresses from the user list.
   - — **From**—Enter your e-mail address.
   - — **Subject**—Enter a subject for the e-mail message.
   - — **Message**—Enter content for the e-mail message.
6. Click **OK**.

Printing a Plan

You can export a plan as a Physical Map in JPG format. You can then print the JPG file from a photo application or a Web browser.

1. Choose **SAN > Export**. The Export dialog box displays, as shown in Figure 100 on page 187.
2. Choose Disk from the **Export To** drop-down list.
3. Choose **Physical Map** and click **Apply**. The plan topology is exported to `<Install_Home>\Client\Data\<sanyymmddhhmmss>`.
4. Open the JPG file in a Web browser or a photo application and print it.

Configuring Zoning

6

This chapter provides instructions for configuring zoning. Zoning defines the communication paths in a fabric. A zone is comprised of a collection of initiator and target ports within the SAN. The ports in a zone can only communicate with other ports in that zone. However, ports can be members of more than one zone. In order to zone devices in a fabric, the fabric's principal switch must be an HP switch and must be discovered and managed through the HAFM.

HAFM performs zoning discovery once at startup, and then once every two hours during routine discovery. If the Zoning dialog box is open, zoning discovery is performed during every polling cycle. It continues to discover at the increased speed for 30 minutes before it returns to the default value. For best results, wait for five discovery cycles after starting the HAFM Appliance before performing zoning. The following zoning features are discussed in this chapter:

Zoning Limitations

HAFM has the ability to configure large zone sets, including up to 1024 zones and 1024 end ports in a single zone set. Table 14 shows the supported limits for the edge switches and directors.

Note: Hard Zoning is enforced upon firmware initialization. Devices not conforming to zoning rules are restricted to their assigned zones.

Table 14: Zoning Parameters Supported Limits

Zoning Parameter	Maximum Value
Number of zone members in a zone	2048
Number of zones in zone set	1024
number of unique zone members in a zone set	2048
Total number of zone members in a zone set (where a zone member can be in multiple zones)	4096
Characters per zoning name	32
Number of unique zone members in HAFM Zoning Library	2048
Number of zones in HAFM Zoning Library	1024
Number of zone sets in HAFM Zoning Library	64
Number of end ports	1024
Number of devices supported (including loop devices)	1024

Note: The supported number of zones is based on a zone name with a maximum of 32 characters. On all edge switches and directors except the Director 2/140, the maximum number of zones decreases if full 64 character names are used. The supported limits are based on two members per zone.

Zone set sizes are affected by the number of zones in the zone set, the length of each zone name, the number of members in each zone, and the Interoperability mode of the fabric. Please consult with HP Professional Services or your support representative if you have questions regarding specific zone set configurations.

Configuring Zoning

Note: Only one appliance should be run at a time (actual appliances performing discovery) or log on conflicts may occur.

To configure zoning for the SAN, perform the following:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101.

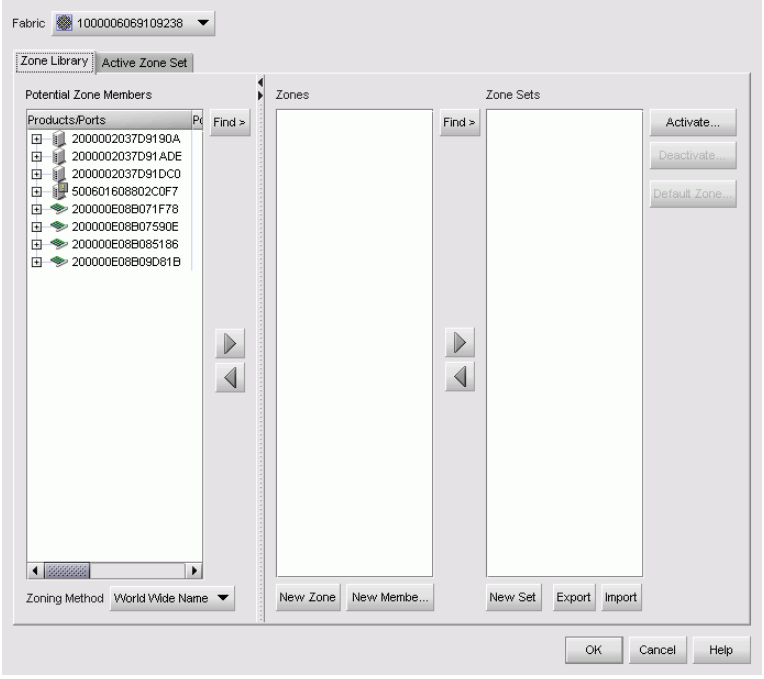


Figure 101: Zoning dialog box

Note: The information displayed in the Zoning dialog box may not be current after 30 minutes. Re-open the dialog box to increase zoning discovery speed and get the current information.

2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Click the **New Zone** button to create a new zone.
5. Rename the zone. See "Zoning Naming Conventions" on page 275 for naming conventions.
6. Choose an option from the **Zoning Method** drop-down list.
7. Choose the member(s) to add to the zone(s) from the **Potential Zone Members** list. Press **CTRL** and click to select more than one member. To add all ports on a device, select the device.
8. Choose the zone(s) to which you want to add members to from the **Zones** list. Press **CTRL** and click to select more than one zone.
9. Click the  button to the right of the **Potential Zone Members** list to add the selected member(s) to the zone(s).
10. Choose zone set(s) to which you want to add zones to from the **Zone Sets** list. Press **CTRL** and click to select more than one zone set.
11. Choose the zones you want to add to the zone set from the **Zones** list. Press **CTRL** and click to select more than one zone.
12. Click the  button to the right of the **Zones** area to add the selected zone(s) to the zone set(s).
13. To activate a zone set, see "Activating a Zone Set" on page 197.
14. Click **OK**.

Note: Activation speeds may differ depending on the hardware vendor and type of zoning used.

When a zone set is activated, only the selected zone set's data is sent to the fabric; zone libraries are never sent to the fabric.

15. Click **OK**.

Creating a New Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.

2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Click **New Zone**. A new zone displays in the **Zones** list.
5. Rename the zone. See "Zoning Naming Conventions" on page 275 for naming conventions.
6. Click **OK**.

Creating a New Member in a Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose the zone(s) to which you want to add members to from the **Zones** list. Press **CTRL** and click to select more than one zone.
5. Click **New Member**. The Add Zone Member dialog box displays, as shown in Figure 102.

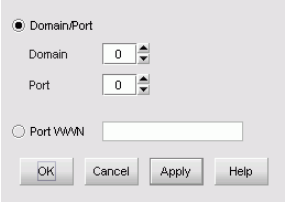


Figure 102: Add Zone Member dialog box

6. You can specify a zone member by its domain ID or world-wide name (WWN).

Note: Zoning by domain and port is only supported in Homogeneous Fabric interop mode.

— To add a zone member by specifying its domain and port, choose **Domain/Port** and enter the domain and port in the appropriate fields. If you add an invalid domain/port value and activate the zone set, the application may initially indicate that the zone has been configured properly. However, a zoning mismatch message displays on the Zoning dialog box after the next discovery pass.

— To add a zone member by its world-wide name, choose **WWN** and enter the WWN in the field. If you add an invalid WWN address and activate the zone set, the application may initially indicate that the zone has been configured properly. However, a zoning mismatch message displays on the **Zoning** dialog box after the next discovery pass.

7. Click **OK** to save your changes and close the Add Zone Member dialog box.
8. Click **OK**.

Note: Library changes are not saved unless you click **OK** on the Zoning dialog box. If you click **Cancel** or the close button (**X**), only zoning changes made to the active zone set is saved. Changes to the active zone set are saved because they have been activated and saved on the switch.

Adding Members to a Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose the zone(s) to which you want to add members to from the **Zones** list. Press **CTRL** and click to select more than one zone.
5. Choose an option from the **Zoning Method** drop-down list.
6. Choose the member(s) to add to the zone(s) from the **Potential Zone Members** list. Press **CTRL** and click to select more than one member. To add all ports on a device, select the device.
7. Click the  button to the right of the **Potential Zone Members** list to add the selected member(s) to the zone(s).
8. Repeat steps 4 through 7 for each member you want to add to the zone.

9. Click **OK**.

Note: Library changes are not saved unless you click **OK** on the Zoning dialog box. If you click **Cancel** or the close button (**X**), only zoning changes made to the active zone set is saved. Changes to the active zone set are saved because they have been activated and saved on the switch.

Creating a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Click **New Set** to create a new zone set.
5. Rename the zone set. See "Zoning Naming Conventions" on page 275 for naming conventions.
6. Press **Enter**.
7. Click **OK**.

Adding Zones to Zone Sets

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose zone set(s) to which you want to add zones to from the **Zone Sets** list. Press **CTRL** and click to select more than one zone set.
5. Click the  button to the right of the **Zones** area to add the selected zone(s) to the zone set(s).
6. Repeat step 4 through step 5 for each zone you want to add to the zone set.
7. To activate a zone set, choose the zone set and click **Activate**.
8. Click **OK**.

Removing a Member from a Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Expand a zone by clicking the + symbol in the **Zones** list.
5. Right-click on a member and click **Remove**. Only the selected zone member is removed. Press **CTRL** and click to select more than one member.
6. Click **OK**.

Removing a Zone from a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Expand a zone set by clicking the + symbol in the **Zones Sets** list.
5. Right-click on a zone and click **Remove**. The zone is removed from the **Zone Set**, and not deleted completely.
6. Click **OK**.

Activating a Zone Set

Note: Activation speeds may differ depending on the hardware vendor and type of zoning used.

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.

4. Choose a zone set from the **Zone Sets** list.
5. Click **Activate**. The Activate Zone Set dialog box displays, as shown in Figure 103.

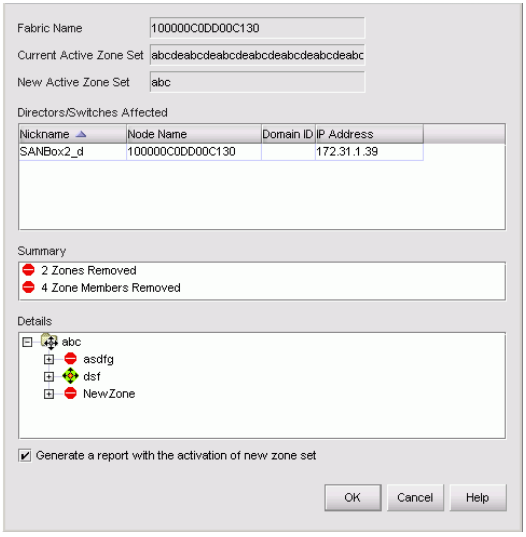


Figure 103: Activate Zone Set dialog box

The Activate Zone Set dialog box displays the names of the fabric, the current active zone set, and the new active zone set. It also lists the number of affected devices and a summary of zone and zone member changed. Verify the information in this dialog box before clicking **OK**.

6. Click **OK**. A Confirmation message displays, as shown in Figure 104.

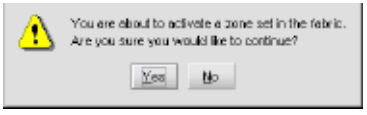


Figure 104: Activate Zone Set confirmation message

7. Click the **Active Zone Set** tab to view the active zone set and all zones within that zone set in the future.

   If the zoning method is not supported, verify that the switch is being managed properly.

Note: Only one appliance should be run at a time (actual appliances performing discovery) or log on conflicts may occur.

8. Click **OK**.

Enabling or Disabling the Default Zone

Enabling the default zone enables the members that are not in zones to see all other members that are not in zones.

1. Choose the fabric for which you want to enable the default zone.
2. Click **Default Zone**.

Note: Default zones are only supported in Homogeneous Fabric interop mode. It is not supported in Open Fabric interop mode. If default zoning is not available, the **Default Zone** button is disabled.

3. Click **OK**.

Deactivating a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Click **Deactivate**. The Deactivate Zone Set dialog box displays, as shown in Figure 105.

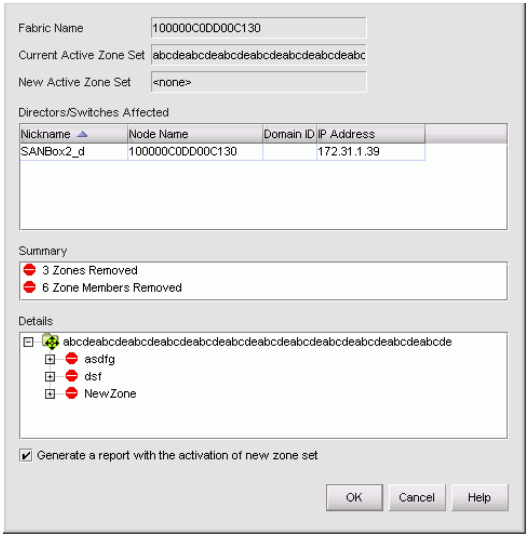


Figure 105: Deactivate Zone Set dialog box

5. The Deactivate Zone Set dialog box displays the names of the current active zone set and lists the new active zone set as "<none>." Verify the information in this dialog box before clicking *OK*.

Note: Be sure to verify the default zone set setting if you want to fully disable zoning. If the default zone is enabled and the active zone set is deactivated, members of the zone may still be able to communicate with each other.

---

6. Click **OK**. The active zone set and all related zones are deactivated.
7. Click **OK**.

Exporting a Zone Set

You can export zone sets as an XML file and then import them into another appliance's zone set library, or to a different zone set library on the current appliance.

Note: You can only export one zone set at a time.

To export a zone set:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose a zone set in the **Zone Sets** list.
5. Click **Export**. The Export Zone Set dialog box displays, as shown in Figure 106.

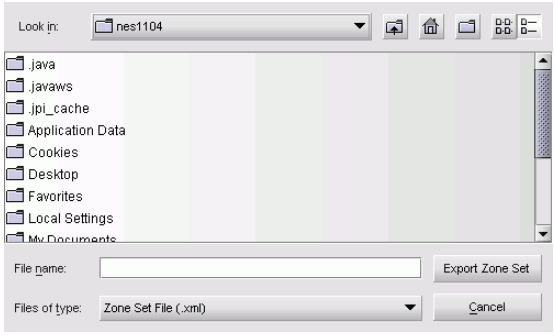


Figure 106: Export Zone Set dialog box

6. If you want to save the document in a different folder, locate and open the folder.
7. Enter a name for the file in the **File name** field.
8. Click **Export Zone Set**. The file is saved to the location you specified.
9. Click **OK**.

Importing a Zone Set

You can import a zone set file into a zone set library.

To import a zone set:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Click **Import**. The Import dialog box displays, as shown in Figure 107.

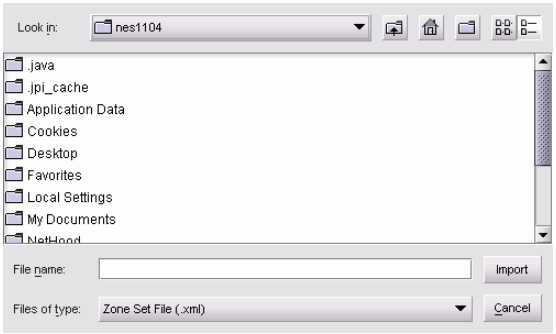


Figure 107: Import Zone Set dialog box

5. Browse to the folder where you exported the zone set.
6. Select the exported XML file and click **Import**.

Note: If the zone set name to be imported already exists in the current zone set library, a warning message displays "Unable to import zoneset. The zoneset name already exists." Change the zone set name and try again.

---

7. Click **OK**.

Zoning Administration

This chapter provides instructions for performing administrative functions with zoning. You can rename, duplicate, delete, and perform other tasks on zones and zone sets.

Renaming a Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click a zone in the **Zones** list and choose **Rename**.
5. Enter the new name for the zone. See "Zoning Naming Conventions" on page 275 for naming conventions.
6. Press **Enter** to save the new name.

Renaming a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click a zone set in the **Zone Sets** list and choose **Rename**.
5. Enter the new name for the zone set. See "Zoning Naming Conventions" on page 275 for naming conventions.
6. Press **Enter** to save the new name.

Replacing Zone Members

There are two methods for replacing a zone member. You can either select the replacement zone member from the **Potential Zone Member** list or you can specify the member's domain/port or WWN.

To replace members by selecting them from the **Potential Zone Member** list, perform the following:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose the member you want to replace from the **Potential Zone Members** list.
5. Click **Find** to the right of the **Potential Zone Members** list to find all instances of the member in the configured zone(s).
6. Click the  button to the right of the **Potential Zone Members** list to unassign the member from the zone(s).
7. Choose the new zone member from the **Potential Zone Members** list.
8. Click the  button to the right of the **Potential Zone Members** list to add the member to the zone(s).
9. Click **OK**.

Manually Replacing Zone Members

To replace zone members manually specifying the member's domain/port or WWN information, perform the following:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click the single zone member you want to replace and choose **Replace**, or right-click in the **Zones** area and choose **Replace All**. The Replace Zone Member dialog box displays, as shown in Figure 108.

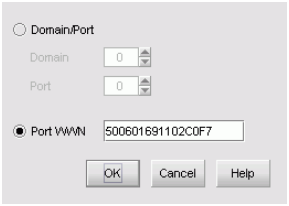


Figure 108: Replace Zone Member dialog box

5. Enter the domain ID and port or the WWN of the replacement member.
6. Click **OK**.

Duplicating a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click a zone set in the **Zone Sets** list and choose **Duplicate** to duplicate the zone set or **Deep Duplicate** to duplicate the zone set and all its zones. The copied zone set displays.
5. Enter a new name for the zone set, if desired. See "Renaming a Zone Set" on page 203.
6. Click **OK**.

Deleting a Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click a zone in the **Zones** list and choose **Delete**.

Note: The zone is deleted without confirmation. If you delete something in error, click **Cancel** to restore it.

5. Click **OK**.

Deleting a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click a zone set in the **Zone Sets** list and choose **Delete**.

Note: The zone set is deleted without confirmation. If you delete something in error, click **Cancel** to restore it.

5. Click **OK**.

Viewing Properties for Zones and Zone Sets

You can view information for zones and zone sets such as name; number of zones, zone sets, or zone members; number of unique zone members; and status.

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Right-click a zone or zone set in the **Zones** or **Zone Sets** list and choose **Properties**.
5. Click **Close** after you have viewed the properties.

Finding Members in a Zone

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose a device or port from the **Potential Zone Members** list and click **Find** to the right of the **Potential Zone Members** list.
5. All found members are highlighted in the **Zones** list.

Finding Zones in a Zone Set

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Zone Library** tab.
4. Choose a zone member or zone from the **Zones** list and click **Find** to the right of the **Zones** list.
5. All zones found are highlighted in the **Zone Sets** list.

Listing Zone Members

1. Choose View All > Levels > All Levels. All levels display on the Product List.
1. Expand a product on the Product List to see the ports.
2. Right-click a port and choose **List Zone Members**. The List Zone Members dialog box displays, as shown in Figure 109. The fabric's nickname, the port's name, and all zone members display.

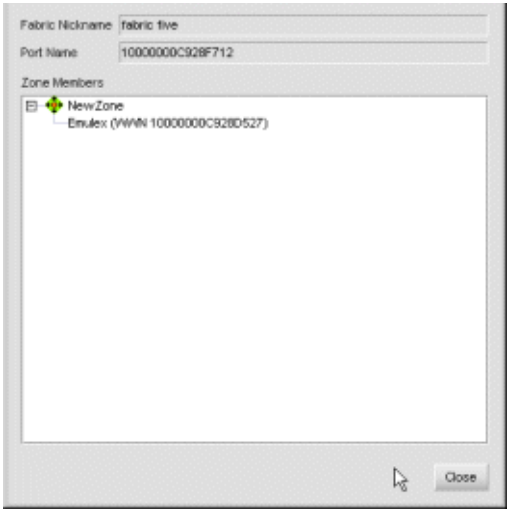


Figure 109: List Zone Members dialog box

3. Click **Close** to close the dialog box.

Saving the Active Zone Set into a Zoning Library

When you manage a switch's zone set via one appliance and then import that switch into a new appliance, any pre-existing zoning information on the switch is not stored on the new appliance until you save the current zone set. Perform the following:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Active Zone Set** tab.
4. Choose the active zoneset.
5. Click **Save As**. The Save Active Zone Set As dialog box displays.
6. Rename the active zone set and click **OK**. This imports the switch's zoning information to the current appliance. You can now manage zones and zone sets through the new appliance.

Comparing Zone Sets

You can compare zone sets against one another. Follow these instructions:

1. Choose **Configure > Zoning**. The Zoning dialog box displays, as shown in Figure 101 on page 192.
2. Choose a fabric from the **Fabric** drop-down list. This sets the fabric to target all zoning actions.
3. Click the **Activate Zone Set** tab.
4. Click **Compare With**. The Select a Zone Set dialog box displays.
5. Choose a zone set and click **OK**. A message displays the comparison results.

Configuring HAFM Through a Firewall

This appendix provides optional procedures for configuring HAFM client and server applications to function across remote networks through a firewall.

This chapter includes:

Polling Client Function

In some cases, a network may use virtual private network (VPN) or firewall technology, which can prohibit communication between Servers and Clients. In other words, a Client can find a Server, appear to log in, but will immediately be logged out because the Server cannot reach the Client. To resolve this issue, the HAFM application will automatically detect the network configuration and run the Client in "polling mode" when necessary.

When the Client is not running in polling mode, the Server calls the client whenever it has new data. When the Client is running in polling mode, the Server will queue up the data and the Client will periodically (approximately every 5 or 10 seconds) check in and get the data. Thus, the original two-way communication is transformed into one-way communication, allowing passage through firewalls.

Configuring for Faster Logins

When a Client attempts to log into a Server, the Server normally calls back to verify communication. In a firewall situation, this call will fail and the Server automatically treats the Client as a "polling" Client. It may take up to 45 seconds for this call-back to fail (worst case). You can configure a polling parameter in Client and Server batch files to let the Server know ahead of time that the Client is a "polling" Client. This skips the call-back from the Server and decreases the login time.

Forcing a Client to Be Polling

To force a specific Client to be a polling Client, edit the `HAFM_co.bat` file and the Client portion of the `HAFM_sc.bat` file, if both files are installed on your computer. These files are in the `HAFM 8.x\bin` directory (typically in `c:\Program Files\HAFM 8.x\bin`).

The `HAFM_sc.bat` file starts both the Client and Server and is installed on a computers with the HAFM appliance software. The `HAFM_co.bat` file starts the Client only and is installed with the Client software.

Add the `-Dsmp.callback.passive` parameter as in the following example. This parameter only affects this client; all other clients can be regular clients.

Note: The following example illustrates the `HAFM_co.bat` file. The portion of this file starting with `rem HAFM Client` is also included in the `HAFM_sc.bat` file. Both files must be modified if they are installed on your computer.

```
setlocal

pushd %~dp0\..

call bin\set_cp.bat

rem HAFM Client

start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH%-Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true
-Dsmp.Mp.max=256 -Dsmp.deployment.prefix=Client/
-Dsmp.callback.passive -Dsmp.flavor=%APP_FLAVOR% Client


rem HAFM Client Debug Mode

rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsun.java2d.noddraw=true -Dsmp.fabricPersistenceEnabled=true
-Dsmp.deployment.prefix=Client/ -Dsmp.debug
-Dsmp.callback.passive ?Dsmp.flavor=%APP_FLAVOR% Client

popd

endlocal
```

Forcing All Clients to Be Polling

To force all Clients communicating with a Server to be treated as polling clients (regardless of the parameters the Clients launch with), edit the `HAFM_sc.bat` file located in the `HAFM 8.x\bin` directory (typically in `c:\Program Files\HAFM 8.x\bin`). Add the `-Dsmp.callback.passive` parameter to the HAFM Server section of the file as in the following example.

```
setlocal

pushd %~dp0\..

call bin\set_cp.bat

.............
```

```
rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xm512m
-Xminf.15 -Xmaxf.35 -classpath %CLASSPATH%
-Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.callback.passive -Dsmp.flavor=%APP_FLAVOR% Server


rem HAFM Server Debug Mode

rem start %JAVA_HOME%\bin\HAFMServerD.exe -server
-Xmx512m -Xminf.15 -Xmaxf.35 -classpath
%CLASSPATH% -Dsun.java2d.noddraw=true -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.debug
-Dsmp.webServer -Dsmp.callback.passive
-Dsmp.flavor=%APP_FLAVOR% Server

.............

:end

popd

endlocal
```

Configuring TCP Port Numbers to Allow Firewall Access

This section provides details about configuring TCP port numbers for RMI Servers and Registries to allow HAFM Client and Server application to function across firewalls.

HAFM Function with RMI at TCP Port Level

The RMI protocol lies between the HAFM application and the TCP/IP layer, as shown in the following table.

Table 15: RMI Protocol Level

HAFM Appliance	HAFM Client
RMI	RMI
TCP/IP	TCP/IP

As shown in Figure 110, the HAFM appliance and Clients communicate with each other through the RMI Server. This is a full-duplex function. However, before the RMI Server on the HAFM Client can communicate with the RMI Server on the HAFM appliance, it must know the TCP port number of the RMI Server. The function of the RMI registry is to communicate this TCP port number to the HAFM Client. Once this is done successfully, communication can take place between the RMI Server on the HAFM appliance and the HAFM Client. (The HAFM appliance obtains the TCP port number of the RMI Server on the Client during initial communications.)

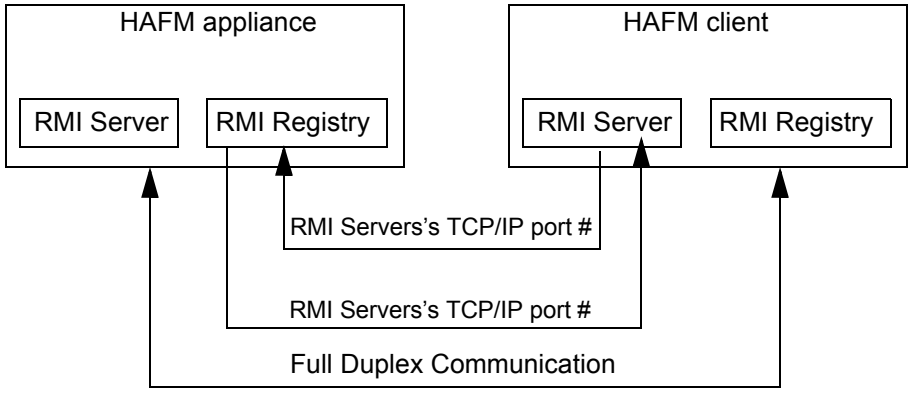


Figure 110: HAFM appliance and client communications

The TCP port numbers of the RMI server are randomly and automatically selected on both the HAFM appliance and Client as a full-duplex function. This poses a major problem for firewalls because they need to know which TCP port numbers to pass through and which numbers to block. Firewalls are configured to block all unknown incoming connections with no mapping of outgoing connections based on a socket part of TCP and IP.

To work around this problem, administrators can "predict" which ports will be used by the Client and Server by configuring these port numbers into appropriate batch files. Using the following procedures depends on how the firewall is set up. Afterward you configure TCP port numbers in the following procedures, the firewall must be configured to unblock the configured port numbers.

- If the firewall prevents the client from connecting to arbitrary ports on the server, then perform both of these procedures:
  - "Forcing Port in RMI Registry" on page 216.
  - "Forcing Server and Client Export Port Number" on page 218.

Note: You must configure both the Server and Client export port numbers.

- If the firewall prevents the server from connecting to arbitrary ports on the client, then configure the export port of the client in "Forcing Server and Client Export Port Number" on page 218.

Note: If the firewall prevents the server from connecting to arbitrary ports on the client, then just configure the export port of the client (`-Dsmp.client.export.port=XXXX`).

Forcing Port in RMI Registry

To force the RMI registry to use a particular TCP port for an RMI server, configure the `Dsmp.registry.port=XXXX` parameter in the `HAFM_sc.bat` file. This file starts both the Client and Server and is installed on a computers with the HAFM appliance software. The file is typically located in `c:\Program Files\HAFM 8.x\bin`. Both the Client and Server areas of the `HAFM_sc.bat` file must have matching parameters. Add a matching parameter to the `HAFM_co.bat` file if, this is installed on your computer. This file starts the Client only and is installed with the Client software.

HAFM_sc.bat File

Edit the HAFM_sc.bat file in the HAFM Server and HAFM Client area to include the parameter `-Dsmp.registry.port=`*`XXXX`*, where *`XXXX`* is any TCP port number not being used by another application. You must place this parameter after the `%CLASSPATH%` parameter as in the following example.

```
setlocal

pushd %~dp0\..

call bin\set_cp.bat

.............

rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.registry.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Server

rem HAFM Server Debug Mode

rem start %JAVA_HOME%\bin\HAFMServerD.exe -server -Xmx512m
-Xminf.15 -Xmaxf.35 -classpath %CLASSPATH%
-Dsmp.Mp.max=512 -Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.debug -Dsmp.webServer
-Dsmp.registry.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Server

:client

rem HAFM Client

start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.registry.port=XXXX
?Dsmp.flavor=%APP_FLAVOR% Client

rem HAFM Client Debug Mode

rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug
-Dsmp.registry.port=XXXX ?Dsmp.flavor=%APP_FLAVOR% Client

:end


popd

endlocal
```

HAFM_co.bat File

```
setlocal

pushd %~dp0\..


call bin\set_cp.bat

..............

rem HAFM Client

start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.flavor=%APP_FLAVOR%
Client


rem HAFM Client Debug Mode

rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug
-Dsmp.registry.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Client
```

Forcing Server and Client Export Port Number

To force the Server and Client to export a specific TCP port number for an RMI server, configure the `-Dsmp.server.export.port=`*`XXXX`* and `-Dsmp.client.export.port=`*`XXXX`* parameters in HAFM_sc.bat and the `-Dsmp.client.export.port=XXXX` in the `HAFM_co.bat` file. These files are typically located in `c:\Program Files\HAFM 8.x\bin`.

Note: If the firewall prevents the server from connecting to arbitrary ports on the client, then just force the export port of the client (`-Dsmp.client.export.port=XXXX`).

The `HAFM_co.bat` file starts both the Client and Server and is installed on a computers with the HAFM appliance software. The file is typically located in `c:\Program Files\HAFM 8.x\bin`. Both the Client and Server areas of the HAFM_sc.bat file must have matching parameters. Add a matching parameter to the `HAFM_co.bat` file if, this is installed on your computer. This file starts the Client only and is installed with the Client software.

HAFM_sc.bat File

Edit the HAFM_sc.bat file in the HAFM Server area to include the parameter `-Dsmp.server.export.port=`*`XXXX`* and the HAFM Client area to include the parameter `-Dsmp.client.export.port=`*`YYYY`*, where *`XXXX`* and *`YYYY`* are any TCP port numbers not being used by another application. Although the server port number *`XXXX`* could match the client port number *`YYYY`*, this is not necessary. If the `HAFM_co.bat` file is installed on your computer, add the `-Dsmp.client.export.port=`*`YYYY`* parameter to that file. Add these parameters after the `%CLASSPATH%` parameter as in the following example.

```
setlocal

pushd %~dp0\..

call bin\set_cp.bat

..............

rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.server.export.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Server

rem HAFM Server Debug Mode

rem start %JAVA_HOME%\bin\HAFMServerD.exe -server -Xmx512m
-Xminf.15 -Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.debug -Dsmp.webServer
-Dsmp.server.export.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Server

:client

rem HAFM Client

start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.client.export.port=YYYY
?Dsmp.flavor=%APP_FLAVOR% Client
```

```
rem HAFM Client Debug Mode

rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug
-Dsmp.client.export.port=YYYY ?Dsmp.flavor=%APP_FLAVOR% Client

:end

popd

endlocal
```

HAFM_co.bat File

```
setlocal

pushd %~dp0\..


call bin\set_cp.bat

..............

rem HAFM Client

start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/-Dsmp.flavor=%APP_FLAVOR% Client


rem HAFM Client Debug Mode

rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug
-Dsmp.client.export.port=YYYY -Dsmp.flavor=%APP_FLAVOR% Client


popd

endlocal
```

Troubleshooting

This appendix provides troubleshooting information as well as zoning information for certain vendors.

Problems with Discovery

Table 16 describes possible problems with discovery and suggested resolutions.

Table 16: Discovery Problems and Resolutions

Problem	Resolution
Discovery is turned off.	Choose **Discover > On**.
Discovered devices are not being displayed.	To correctly discover all SAN devices, specify each device in the Out-of-Band dialog box, either by the individual IP address or by subnet. 1. Choose **Discover > Setup**. 2. Add, change, and remove IP addresses, as necessary. See "Configuring IP Addresses and Community Strings" on page 70 for instructions. 3. Select IP addresses from the **Available Addresses** table and add them to the **Selected Subnets** or **Selected Individual Addresses** tables by clicking the buttons. If you add addresses to the **Selected Subnets** table, choose a **Method** (Broadcast or Sweep). 4. Click **OK**.
	Ensure that you've selected to view the fabric that includes the discovered devices.
	Ensure that only one copy of the application is being used to monitor and manage the same devices in a subnet.

Table 16: Discovery Problems and Resolutions (Continued)

Problem	Resolution
Broadcast request blocked by routers.	**Resolution 1:** If you know the IP addresses and the addresses are not in the **Available Addresses** pane: 1. Choose **Discover > Setup**. 2. Click **Add**. 3. Enter data in the dialog box. 4. Click **OK**. 5. Repeat steps step 1 through step 4 until all your addresses are available. 6. Select the IP addresses you would like to discover in the **Available Addresses** pane. 7. Click the button to move your choices to the **Selected Individual Addresses** pane. 8. Click **OK**. **Resolution 2:** If you know the IP addresses and the addresses are listed in the **Available Addresses** pane: 1. Choose **Discover > Setup**. 2. Select the IP addresses you would like to discover in the **Available Addresses** pane. 3. Click the button to move your choices to the **Selected Individual Addresses** pane. 4. Click **OK**. **Resolution 3:** This method significantly increases your discovery time. If you don't know the specific IP addresses: 1. Choose **Discover > Setup**. 2. Click on the **Method** column for the selected subnet in the **Selected Subnets** pane and choose **Sweep**. 3. Click **OK**.

Table 16: Discovery Problems and Resolutions (Continued)

Problem	Resolution
Discovery time is excessive.	**Resolution 1**: 1. Choose **Discover > Setup**. 2. Click on the **Method** column in the **Selected Subnets** pane and choose **Broadcast**. 3. Click **OK**. **Resolution 2:** Decrease the SNMP time-out to decrease the discovery time.
Can't open an Element Manager for an HP device.	Ensure that only one copy of the application is being used to monitor and manage the device. Only one copy of the application can be used to monitor and manage the same devices in a subnet.

Problems with Products

Table 17 describes possible product problems and suggested resolutions.

Table 17: Product Problems and Resolutions

Problem	Resolution
HBAs not connected to SAN.	Check your physical cables and connectors.
Switches not connected to Ethernet.	Check your physical cables and connectors.
Switches not connected to SAN.	Check your physical cables and connectors.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You may have attempted to disable Fabric Binding through the Fabric Binding dialog box while Enterprise Fabric Mode was enabled. Disable the Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Fabric Binding.

Problems with Addresses

Table 18 describes possible problems with addresses and suggested resolutions.

Table 18: Address Problems and Resolutions

Problem	Resolution
No subnets or addresses selected.	1. Choose **Discover > Setup**. 2. Click on the subnet or individual address you would like to discover in the **Available Addresses** pane. 3. Click the button to move your choice to the **Selected Subnets** pane, or to the **Selected Individual Addresses** pane. 4. Click **OK**.
Wrong IP addresses selected.	1. Choose **Discover > Setup**. 2. Verify that the IP addresses in the **Selected Subnets** and **Selected Individual Addresses** panes are the correct current addresses for the SAN. 3. Click **OK**.
Wrong community strings are selected.	1. Choose **Discover > Setup**. 2. Select an IP address. 3. Click **Change**. 4. Select the desired community strings. 5. Click **OK**.

Miscellaneous Problems

Table 19 describes possible miscellaneous problems and suggested resolutions.

Table 19: Miscellaneous Problems and Resolutions

Problem	Resolution
"Code Execution Error: Array Index Out-Of-Bounds" displays.	Retry the command or action. If the problem persists, contact Customer Support.
"Code Execution Error: Internal Exception" displays.	Retry the command or action. If the problem persists, contact Customer Support.
"Code Execution Error: Missing Property File" displays.	Retry the command or action. If the problem persists, contact Customer Support.
"Code Execution Error: Invalid Product Type" displays.	Retry the command or action. If the problem persists, contact Customer Support.
The Server doesn't seem to be starting.	Examine the Server log (*<Install_Home>\Server\Universe_Home\TestUniverse_Working\EventStorageProvider\event.log*) for diagnostic information.
Server to Client communication is inhibited.	In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between servers and clients. In other words, a client can find a server, appear to log in, but is immediately logged out because the server cannot reach the client. To resolve this issue, the application automatically detects the network configuration and run the client in "polling mode" when necessary. When the client is not running in polling mode, the server calls the client whenever it has new data. When the client is running in polling mode, the server queues up the data and the client periodically (approximately every 5 or 10 seconds) checks in and gets the data.
Data and settings not imported during installation.	Open an MS-DOS window and enter the following script at the command line: Install_Service <startstatus> <runnow> where **startstatus** parameter is *manual* or *auto* and **runnow** parameter is *true* or *false*

Table 19: Miscellaneous Problems and Resolutions (Continued)

Problem	Resolution
Windows service does not display correctly in the Computer Management (Windows 2000) or Service Control Manager (Windows NT) window.	If you installed or uninstalled the Win32 service while the Computer Management or Service Control Manager window was open, the service does not display. Close the window and re-open it to see the changes.
An error displayed stating that the application failed to setup the *serverinit.txt* or *./license* file.	Delete the *<Install_Home>\Server\serverinit.txt* file or the *<Install_Home>\Server\Config\Other\ ./license* file and rerun the installer.
The product does not install on a Windows system.	Verify that the system has 100 MB available on the C drive. The program requires 100 MB for installation, but only 50 MB to run.
Mapping a loop to a hub causes the loop group and the outermost portion of the topology's background group color or layout format to revert to the default.	Make the background and/or layout changes after mapping the loop to the hub.
The hyperlinks in a report are broken.	Hyperlinks in reports are only active as long as the source data is available.
When the client application is started on an HP-UX machine, the exception "java.lang.OutOfMemoryError: unable to create new native thread" displays in thread "main."	The following two HP-UX 11.0 kernel parameters are set too low for most *Java* applications. Usually you see this problem as a Java Out of Memory error. To resolve the issue, edit the parameter limits as mentioned below. **max_thread_proc** The maximum number of threads allowed in each process. The minimum value (and default) is 64, often too low for most *Java* applications. Set the value of the max_thread_proc higher (for example, 1024) than the expected maximum number of simultaneously active threads. The maximum value is the value of nkthread. **nkthread** The total number of kernel threads available in the system. This parameter is similar to the nproc tunable except that it defines the limit for the total number of kernel threads able to run simultaneously in the system. The value must be greater than nproc. The default is approximately twice that of nproc. The maximum is 30000.

Table 19: Miscellaneous Problems and Resolutions (Continued)

Problem	Resolution
The system reboots or is unable to gather SNMP information.	Multiple SNMP calls are being sent to a device that can't handle the constant requests for information. To resolve this issue, verify that the devices you are discovering are not being discovered by another appliance. Discovering devices using multiple appliances may result in errors.
A report failed to generate due to memory constraints.	Generate a fewer number of reports at one time.
Receiving error "Compatibility between <TARGET VERSION> and <CURRENT VERSION> is unknown. Do you want to continue?"	Firmware files are included in the upgrade process, but release rules are not. Since release rules are required when sending another firmware version to a switch, this error results. To fix this problem, add the latest firmware file to the firmware library. This also adds the new release rules and resolve the problem.
Error occurs when trying to delete a nickname.	Once assigned, a nickname cannot be deleted and left blank.

Problems with Zoning

The following section states some possible issues and recommended solutions for zoning errors.

Table 20: Zoning Problems and Resolutions

Problem	Resolution
Receiving zoning errors.	Verify that you did not configure zoning on a non-principal switch.
The application is not performing zoning discovery very often.	Zoning discovery is performed once at startup, and then once every two hours during routine discovery. If the Zoning dialog box is open, zoning discovery is performed during every polling cycle. It continues to discover at the increased speed for 30 minutes before it returns to the default value.
When activating a large zone set on a two-switch fabric on UNIX platforms, an error message displays stating "Failed to perform the requested zoning action: Failed to zone due to exception COM.hp.hafmecc.HafmUnavailableException."	Although the error message states that the requested zoning action failed, the zone set correctly activated. Wait for the next zoning polling to occur. This issue only occurs on UNIX systems.
Zoning activation message displays for a long time, but zone set is not activated.	Telnet zoning can take a long time. To improve speed, open the Discover Setup dialog box and add the HAFM IP address for HP switches to the **Selected Individual Addresses** list.
When opening the Zoning dialog box from a particular switch or fabric, the message "Cannot zone the selected device or fabric" displays.	The application may not have been able to log in to the fabric due to another active session. Verify that there isn't another active session. The application may not support zoning on any of the discovered products.

Information and Error Messages

This appendix lists information and error messages that display in pop-up message boxes from the HP StorageWorks *HA-Fabric Manager* (*HAFM*) application.

Table 21: HAFM Messages

Message	Description	Action
A zone must have at least one zone member.	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone using the Modify Zone dialog box.
A zone set must have at least one zone.	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set using the Modify Zone dialog box.
All alias, zone, and zone set names must be unique.	When creating a new alias, zone, or zone set, the name must be unique.	At the New Zone dialog box, choose a unique name for the new alias, zone, or zone set.
All zone members are logged.	Attempt was made to display all zone members not logged in using the **Zone Set** tab, but all members are currently logged in.	Informational message.
An HAFM application session is already active from this workstation.	Only one instance of the *HAFM* application is allowed to be open per remote workstation.	Close all but one of the *HAFM* application sessions.
Are you sure you want to delete this network address?	The currently-selected network address will be deleted.	Click **Yes** to delete or **No** to cancel.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click **Yes** to delete the nickname or **No** to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click **Yes** to delete the product or **No** to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click **Yes** to delete the user or **No** to cancel the operation.
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click **Yes** to delete the zone or **No** to cancel the operation.
Are you sure you want to delete this zone set?	The selected zone set will be deleted from the zone library.	Click **Yes** to delete the zone set or **No** to cancel the operation.
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click **Yes** to overwrite or **No** to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click **Yes** to delete the members or **No** to cancel the operation.
Cannot add a switch to a zone.	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding World Wide Name for the device you want to add to the zone.
Cannot connect to management server.	The *HAFM* application at a remote workstation could not connect to the HAFM appliance.	Verify the HAFM appliance internet protocol (IP) address is valid.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Cannot delete product.	The selected product cannot be deleted.	Verify the HAFM appliance-to-product link is up. If the link is up: ■ The HAFM appliance may be busy. ■ Another Element Manager instance may be open. ■ You may not have permission to delete the product.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You attempted to disable Fabric Binding through the Fabric Binding dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in the *HAFM* application before disabling Fabric Binding.
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route between devices that are attached to switches or directors managed by a different HAFM appliance.	Make sure devices named in Show Routes dialog box are attached to products managed by this HAFM appliance.
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Edge Switch 2/16s, Edge Switch 2/24s, Edge Switch 2/32s, Director 2/64s, or Director 2/140s.
Cannot display route. Device is not a member of a zone in the active zone set.	You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.
Cannot display route on one switch fabric.	You cannot show routes between end devices in a fabric when configuring **Show Routes** (**Configure** menu).	Error displays when attempting to show routes on a fabric with only one switch. Configure **Show Routes** on a multi-switch fabric.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Cannot display route. error 9.	An internal error has occurred while trying to view routes.	Contact the next level of support to report the problem.
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then modify the name through the Modify Zone Set dialog box.
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then modify the name through the Modify Zone Set dialog box.
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM appliance-to-product link is up. If the link is up: ■ The HAFM appliance may be busy. ■ Another Element Manager instance may be open. ■ You may not have permission to modify the product.
Cannot perform operation. Fabric is unknown.	This message displays if no switches in the fabric are connected to the HAFM appliance.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM appliance and retry the operation.
Cannot perform operation. The list of attached nodes is unavailable.	This message displays when attached nodes are unavailable and you attempt to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Cannot retrieve current SNMP configuration.	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
Cannot save current SNMP configuration.	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.
Cannot set write authorization without defining a community name.	An SNMP community name has not been configured.	Enter a valid community name in the Configure SNMP dialog box.
Cannot show zoning library. No fabric exists.	You cannot show the zoning library if no fabric exists. You must have identified a switch or director to the *HAFM* application for a fabric to exist.	Identify an existing switch or director to the *HAFM* application using the New Product dialog box.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or **Cancel** to cancel the operation.
Connection to management server lost.	The connection to the remote HAFM appliance has been lost.	Log in to the HAFM appliance again through the HAFM Log In dialog box.
Connection to management server lost. Click OK to exit application.	The *HAFM* application at a remote workstation lost the network connection to the HAFM appliance.	Re-start the *HAFM* application to connect to the HAFM appliance.
Could not export log to file.	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Default zoning is not supported in Open Fabric Mode.	A default zone cannot be enabled when the product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers.	Change the Interop Mode from Open Fabric to Homogeneous using the Configure Fabric Parameters dialog box. You can also redefine zone members by the device WWN.
Device is not a member of a zone in the active zone set.	The selected device is not a member of a zone in the active zone set and therefore cannot communicate with the other devices in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.
Download complete. Click OK and start the HAFM.	Download of HAFM and the Element Manager is complete.	Start the *HAFM* application to continue.
Duplicate community names require identical write authorizations.	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
Duplicate Fabric Name.	The specified fabric name already exists.	Choose another name for the fabric.
Duplicate name in zoning configuration. All zone and zone set names must be unique.	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
Duplicate nickname in nickname configuration.	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.
Duplicate World Wide Name in nickname configuration.	A World Wide Name can be associated with only one nickname.	Modify (to make it unique) or delete the selected World Wide Name.
Duplicate zone in zone set configuration.	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Duplicate zone member in zone configuration.	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
Element Manager instance is currently open.	A product cannot be deleted while an instance of the Element Manager is open for that product.	Close the Element Manager, then delete the product.
Enabling this zone set will replace the currently active zone set. Do you want to continue?	Only one zone set can be active. By enabling the selected zone set, the current active zone set will be replaced.	Click **OK** to continue or **Cancel** to end the operation.
Error connecting to switch.	While viewing routes, the HAFM appliance was unable to connect to the switch. The switch failed or the switch-to-HAFM appliance Ethernet link failed.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The *HAFM* application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.
Error removing zone or zone member.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the *HAFM* application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Fabric Log will be lost once the fabric unpersists. Do you want to continue?	When you unpersist a fabric, the corresponding fabric log is deleted.	Click **Yes** to unpersist the fabric or **No** to cancel the operation.
Fabric member could not be found.	A fabric member does not exist when the application prepared to find a route, find a route node, or gather route information on that fabric member.	Ensure the product is incorporated into the fabric and retry the operation. If the problem persists, contact the next level of support.
Fabric not persisted.	You attempted to refresh or clear the log, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted.	Click **OK** to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
File transfer aborted.	You aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.
HAFM error <error number 1 through 8 >.	The *HAFM* application encountered an internal error (1 through 8 inclusive) and cannot continue operation.	Contact the next level of support to report the problem.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Management server could not log you on. Verify your username and password.	An incorrect username or password (both case sensitive) was used while attempting to log in to the *HAFM* application.	Verify the username and password with the customer's network administrator and retry the operation.
Management server is shutting down. Connection will be terminated.	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
Invalid name.	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Choose a valid name and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number. Valid ports are (0-< nn >).	You have specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus 1. For example, for a switch with 32 ports, the valid port range is 0–31.
Invalid product selection.	At the New Product dialog box, an invalid product was selected.	Choose a valid product and retry the operation.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Invalid request.	Three conditions result in this message: ■ You tried to add or modify a product from **Product View** and the network address is already in use. (Network addresses must be unique.) ■ You tried to create a new user with a username that already exists. (A username must be unique.) ■ You tried to delete the default Administrator user. (The default Administrator user cannot be deleted.)	Choose the action that is appropriate to the activity that caused the error: ■ Network address: Specify a unique network address for the product. ■ username: Specify a unique username for the new user ID. ■ Do not delete the default Administrator user.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.
Invalid World Wide Name.	The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a World Wide Name using the correct format.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Invalid World Wide Name or nickname.	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
Invalid World Wide Name. Valid WWN format is: xx:xx:xx:xx:xx:xx:xx:xx.	The specified World Wide Name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Retry the operation using a valid WWN or nickname.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.
Limit exceeded.	You cannot add a new product or user to *HAFM* application if the maximum number of that resource already exists on the system.	Delete unneeded products or users from the system, before attempting to add any new ones.
No address selected.	You cannot complete the operation because an address has not been selected.	Choose an address and retry the operation.
No attached nodes selected.	An operation was attempted without an attached node selected.	Choose an attached node and try the operation again.

Table 21: HAFM Messages (Continued)

Message	Description	Action
No management server specified.	An HAFM appliance is not defined to the *HAFM* application.	At the HAFM 8 Log In dialog box, type an appliance name in the **Server Name** field and click **Login**.
No nickname selected.	No nickname was selected when the command was attempted.	Choose a nickname and try again.
No Element Managers installed.	No director or switch Element Manager is installed on this workstation.	Install the appropriate Element Manager to this workstation.
No routing information available.	No information is available for the route selected.	Choose a different route and try the operation again.
No user selected.	A user was not selected when the command was attempted.	Choose a user and try again.
No zone member selected.	A zoning operation was attempted without a zone member selected.	Choose a zone member and try the operation again.
No zone selected.	A zoning operation was attempted without a zone selected.	Choose a zone and try the operation again.
No zone selected or zone no longer exists.	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Choose a zone and try the operation again.
No zone set active.	A zone set cannot be deactivated if there are no active zones.	Informational message only—no action is required.
No zone set selected.	A zoning operation was attempted without a zone set selected.	Choose a zone set and try the operation again.

Table 21: HAFM Messages (Continued)

Message	Description	Action
No zone set selected or zone set no longer exists.	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Choose a zone set and try the operation again.
Only attached nodes can be displayed in this mode.	You cannot display unused ports when adding ports by World Wide Name.	Change the add criteria to Add by Port.
Password and confirmation don't match.	Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
Remote sessions are not allowed from this network address.	Only IP addresses of remote workstations specified at the Remote Access dialog box are allowed to connect to the HAFM appliance.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.
Remote session support has been disabled.	The connection between the specified remote workstation and the HAFM appliance was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the Remote Access dialog box.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later.
Route data corrupted.	The information for this route is corrupt.	Try the operation again. If the problem persists, contact the next level of support.
Route request timeout.	The Show Route request timed out.	Try the operation again. If the problem persists, contact the next level of support.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Routing is not supported by the switch.	This switch or director does not support the Show Routes feature.	Choose a different switch or director to show the route.
SANtegrity Feature not installed. Please contact your sales representative.	You selected **Fabric Binding** or **Enterprise Fabric Mode** from the **Fabrics** menu. These selections are not enabled because the optional SANtegrity binding feature is not installed.	Install the SANtegrity Binding feature to use Fabric Binding or enable Enterprise Fabric Mode.
Select alias to add to zone.	An alias was not selected before clicking **Add**.	Choose an alias before clicking **Add**.
Selection is not a World Wide Name.	The selection made is not a World Wide Name.	Choose a valid World Wide Name before performing this operation.
Server shutting down.	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Switch is not managed by HAFM.	The selected switch or director is not managed by the *HAFM* application.	Choose a different switch or director.
The Administrator user cannot be deleted.	The administrator user is permanent and cannot be deleted from the Configure Users dialog box.	Informational message only—no action is required.

Table 21: HAFM Messages (Continued)

Message	Description	Action
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but a switch already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the Add Detached Switch dialog box.
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager and cannot perform the requested operation.	Wait until the process completes, then perform the operation again.
The link to the managed product is not available.	The Ethernet connection between the HAFM appliance and managed product is down or unavailable.	Establish and verify the network connection.
The maximum number of aliases has already been configured.	The maximum number of aliases allowed was reached.	Delete an existing alias before adding a new alias.
The maximum number of management server network addresses has already been configured.	The number of HAFM appliance IP addressees that can be defined to the *HAFM* application has already been configured.	Delete an existing IP address before adding a new address.
The maximum number of members has already been configured.	The maximum number of unique members is 4097. The maximum number of members is 8192.	Delete an existing zone member before adding a new zone member.

Table 21: HAFM Messages (Continued)

Message	Description	Action
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the *HAFM* application was reached.	Delete an existing nickname before adding a new nickname.
The maximum number of open products has already been reached.	The maximum number of open switches allowed was reached.	Close an *Element Manager* session (existing open product) before opening a new session.
The maximum number of products has already been configured.	The number of managed HP switches (48) that can be defined to the *HAFM* application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of managed HP switches of this type (48) that can be defined to the *HAFM* application was reached.	Delete an existing product of this type before adding a new product.
The maximum number of remote network addresses has already been configured.	A maximum number of eight IP addresses for remote workstations can be configured at the Session Options dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of users has already been configured.	The number of users (32) that can be defined to the *HAFM* application was reached.	Delete an existing user before adding a new user.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.

Table 21: HAFM Messages (Continued)

Message	Description	Action
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.
The software version on this management server is not compatible with the version on the remote management server.	A second HAFM appliance (client) connecting to the HAFM appliance must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM appliance.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected fabric log is no longer available because the fabric has been unpersisted.	To start a new log for the fabric, persist the fabric through the Persist Fabric dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.
This product is not managed by this management server.	The product selected is not managed by this HAFM appliance.	Choose a product managed by this HAFM appliance or go to the HAFM appliance that manages the affected product.

Table 21: HAFM Messages (Continued)

Message	Description	Action
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	You attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric.	Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected.
This World Wide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but an entry already exists in the Fabric Membership List with the same World Wide Name (WWN).	Enter a unique World Wide Name for the switch in the Add Detached Switch dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.
You do not have a compatible version of the management server software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click OK to install a compatible version.	The *HAFM* application version running on the HAFM appliance differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM appliance.	Download a compatible version of the *HAFM* application to the remote workstation (client) using the Web install procedure.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required using the Configure Users dialog box.

Table 21: HAFM Messages (Continued)

Message	Description	Action
You must define an SMTP server address.	An SMTP server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the Configure E-Mail dialog box.
You must define at least one E-mail address.	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the Configure E-Mail dialog box.
You must define at least one remote network address.	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the Remote Access dialog box.
You must download the HAFM client via the web install.	An attempt was made to download the *HAFM* application to a remote workstation (client) using an improper procedure.	Download a compatible version of the *HAFM* application to the remote workstation (client) using the Web install procedure.
Zones configured with port numbers are ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names.	Informational message only–no action is required.
Zones must be defined before creating a zone set.	You cannot create a zone set without any zones defined for *HAFM*.	Define zones using the New Zone dialog box.
Zoning by port number is ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through World Wide Names.	Informational message only–no action is required.

Table 21: HAFM Messages (Continued)

Message	Description	Action
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if *HAFM* is in Open Fabric Mode.	Either define zones by WWN of device or change to Homogeneous Fabric mode in the Configure Operation Mode dialog box of the Element Manager.
Zoning name already exists.	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

Configuring Remote Workstations

This appendix describes the procedures for installing the *HAFM* application on a remote workstation. To run HAFM on a remote workstation, you must first download and install the *HAFM* application from the HAFM appliance.

The figures in this chapter show Netscape Navigator as the Internet browser; however, it is acceptable to use Microsoft Internet Explorer during these procedures. The following sections discussed in this chapter:

Configuring Windows Systems

This section describes the procedures for installing HAFM on a remote workstation running Windows 2000, Windows NT, or Windows XP.

Requirements

The download and installation process requires the use of a personal computer (PC) with the following minimum system requirements:

- Operating system (one of the following):
  - Windows 2000 Professional (with service pack 3)
  - Windows NT 4.0 (with service pack 6a)
  - Windows XP (with service pack 1a)
- 1 gigahertz (GHz) Pentium III processor
- 512 megabyte (MB) random access memory (RAM) memory
- 350 MB available disk space
- Video card supporting 256 colors at 800 x 600 resolution
- Ethernet network adapter
- Java-enabled Internet browser, such as Microsoft Internet Explorer (version 4.0 or later) or Netscape Navigator (version 4.6 or later)

Newer versions of the High Availability Fabric Manager or Element Managers installed on the HAFM appliance automatically download when the remote clients log in to the appliance.

Installation Procedure

To install the HAFM on a remote workstation:

1. Open a World Wide Web (WWW) browser.
2. Type the address of the HAFM appliance in the **Location** (or **Address**) box on the browser, then press **Enter**.

   Obtain the HAFM appliance address from your network administrator

   The **HP StorageWorks HAFM remote client installation** screen displays. Figure 111 shows the upper portion of this page.

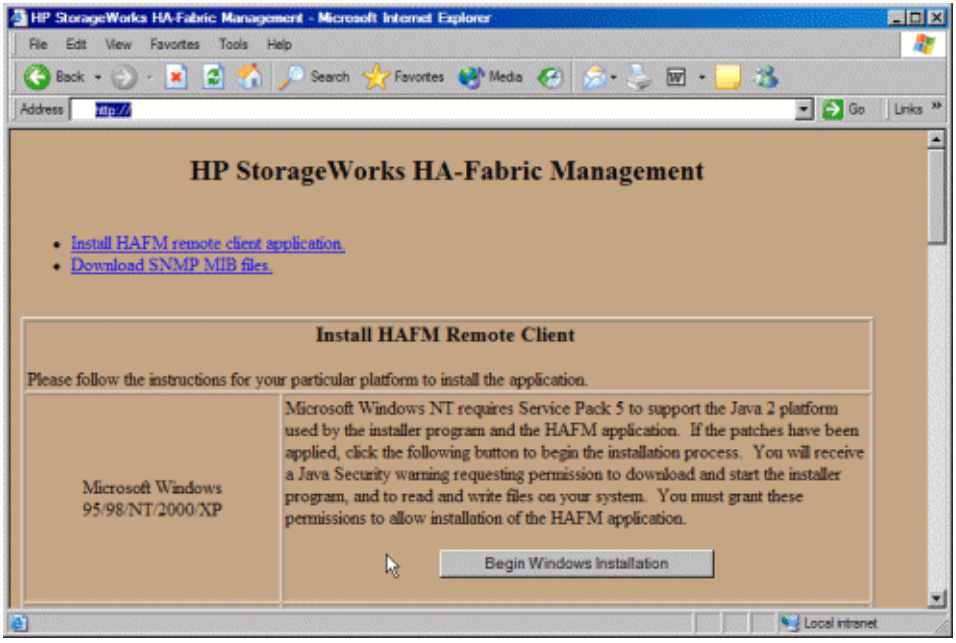


Figure 111: Remote Client Installation screen

3. On the page, click **Begin Windows Installation** to begin the installation process. If you have read the security agreement information and wish to continue, click **Yes**. The **HP High Availability Fabric Manager Available Installers** page displays, as shown in Figure 112.

Figure 112: Available Installers page

4. On the **HP High Availability Fabric Manager Available Installers** page, click **Download**. The File Download dialog box displays, as shown in Figure 113.

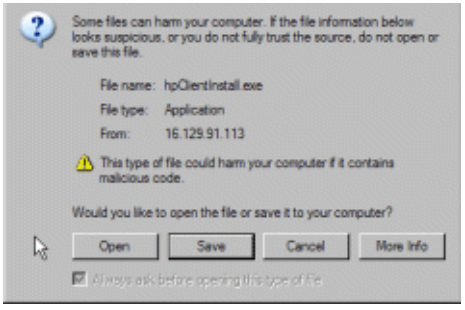


Figure 113: File Download dialog box

5. Click Open. The system begins downloading the HAFM installer. When the download is complete, the **Introduction** screen displays.

6. Click **Next**. At any time, you may return to the previous page by clicking **Previous** or quit the Installer by clicking **Cancel**. The **License Agreement** screen displays,.
7. If you have read the license agreement and agree to accept the terms, click **I accept the terms of the License Agreement**.
8. Click **Next**. The **Important Information** screen displays,.
9. Click **Next**. The **Choose Install Folder** screen displays.
10. Select a folder on the remote workstation in which to store the HAFM software. You can accept the default location, type in the path to a new location, or click **Choose** to browse for an appropriate location. Click **Restore Default Folder** to change the location back to the default folder.
11. Click **Next**.

    If the HAFM is already installed on the system, you are prompted to uninstall the existing version. If you want to uninstall the existing software, click **Yes** and press **Next**. When the Uninstall HAFM window displays, click **Uninstall**. When the **Uninstall Complete** screen displays, click **Quit**.

    The **Choose Shortcut Location** screen displays.
12. Select a shortcut location. The options for the location of HAFM icons are:
    - **In a new Program Group**—Adds a new program group on the **Start** menu for the HAFM.
    - **In an existing Program Group**—Enables you to choose from existing program groups on the **Start** menu for the HAFM.
    - **In the Start Menu**—Puts the **HAFM** icon on the initial **Start** menu.
    - **On the Desktop**—Puts the HAFM icons on the Windows desktop.
    - **Other**—Enables you to choose any location on your hard drive or network for the HAFM files.
    - **Don't create icons**—Prevents the installation from creating an icon for the HAFM.

    The **Create Icons for All Users** check box can be enabled for some of the shortcut options but not all. If the check box is enabled, the appropriate HAFM icons are placed on the desktop and in the `Programs` folder of every Windows user. If the check box is cleared, the icons are created only for the current user and are not visible for other user IDs.
13. Click **Next** to begin the installation. The **Pre-Installation Summary** screen displays.

14. Review the installation information and click **Install**.

    The progress of the installation is tracked on the **Installing HP StorageWorks HAFM** screen.

    When the installation is complete, the **Install Complete** dialog box displays.

15. Click **Done** to close the **Install Complete** dialog box.

Running the High Availability Fabric Manager

1. If you chose icons to be created in step 12 of the installation procedure, access the icon installed in the windows **Start** menu or desktop to run HAFM.
2. If you did not create any icons in step 12 of the installation procedure, access the HAFM folder (default location: `<Install_Home>/bin/)`.
3. Double-click the file `HAFM_coo.bat` to run the HAFM program.

Configuring Solaris Systems

This section describes the procedures for installing HAFM on a remote Solaris workstation.

Requirements

The download and installation process requires the use of a workstation with the following minimum system requirements:

- Solaris version 7.0
- UltraSPARC-IIi processor
- 512 megabyte (MB) random access memory (RAM) memory
- 350 MB available disk space
- Video card supporting 256 colors at 800 x 600 resolution
- Network connection
- Internet browser, such as Microsoft Internet Explorer (version 4.0 or later) or Netscape Navigator (version 4.6 or later)

Newer versions of the HAFM or Element Managers installed on the HAFM appliance automatically download when the remote clients log in to the appliance.

Installation Procedure

To install the HAFM on a remote workstation:

1. Open a World Wide Web (WWW) browser.
2. Type the address of the HAFM appliance in the **Location** (or **Address**) field of the browser, then press **Enter**.

   Obtain the HAFM appliance address from your network administrator

   The **HP StorageWorks HAFM** page displays. Figure 111 illustrates a partial page with the Windows installation section.
3. On the page, click **Begin Solaris Installation** to begin the installation process. If you have read the security agreement information and wish to continue, click **Yes**. The **HP High Availability Fabric Manager Available Installers** page displays, as shown in Figure 112.

4. On the **HP High Availability Fabric Manager Available Installers** page, click **Download**. The File Download dialog box displays, as shown in Figure 113.
5. Click Open. The system begins downloading the HAFM installer. When the download is complete, the **Introduction** screen displays.
6. Click **Next**. At any time, you may return to the previous page by clicking **Previous** or quit the Installer by clicking **Exit**. The **License Agreement** screen displays.
7. If you have read the license agreement and agree to accept the terms, click **I accept the terms of the License Agreement**.
8. Click **Next**. The **Important Information** screen displays.
9. Click **Next**. The **Choose Install Folder** screen displays.
10. Choose a folder on the remote workstation in which to store the HAFM software. You can accept the default location, type in the path to a new location, or click **Choose** to browse for an appropriate location. Click **Restore Default Location** to change the location back to the default.
11. Click **Next**. The **Choose Shortcut Location** screen displays.

Note: If the HAFM is already installed on the system, you are prompted to uninstall the existing version of the HAFM. If you want to uninstall the existing software, click **Yes** and press **Next**. In the Uninstall High Availability Fabric Manager window, click **Uninstall**. When the uninstallation process is done, click **Quit**.

---

12. Select a shortcut location. The options for the location of HAFM links are:
    - **In your home folder**—Adds a new program group on the **Start** menu for the HAFM.
    - **Other**—Enables you to choose any location on your hard drive or network for the HAFM files.
    - **Don't create links**—Prevents the installation from creating a link for the HAFM.
13. Click **Next** to begin the installation. The **Pre-Installation Summary** screen displays.
14. Review the installation information and click **Install**.

The progress of the installation is tracked on the **Installing HP StorageWorks HAFM** screen.

15. If desired, enable the **Start the High Availability Fabric Manager** check box to immediately open the HAFM. Click **Done** to close the **Install Complete** dialog box.

Running the High Availability Fabric Manager

Run the HAFM program from the directory in which you saved it (the default is a subdirectory named `HAFM` in your home directory).

1. In the Terminal window, type `cd HAFM`.
2. Press **Enter**.
3. Then type `HAFM_Manager`.
4. Press **Enter**. The *HAFM* application opens.

Configuring HP-UX, AIX, and Linux Systems

This appendix describes the procedures for installing the HAFM on a remote HP-UX, AIX, or Linux workstation.

Note: The figures in this appendix show Netscape Navigator as the internet browser; however, you can also use Microsoft Internet Explorer for this installation procedure.

Requirements

The download and installation process requires the use of a PC with the following minimum system requirements:

- Operating system (one of the following):
  - HP-UX 11.0a
  - AIX minimum version 4.3.3
  - Red Hat 7.3
- Processor:
  - 400 MHz HA PA-RISC
  - 333 MHz Power3-II
  - 1 GHz Intel Pentium III
- 512 MB RAM
- 350 MB disk space
- Video card supporting 256 colors at 800 x 600 resolution
- Ethernet network adapter
- Java-enabled Internet browser, such as Microsoft Internet Explorer (version 4.0 or later) or Netscape Navigator (version 4.6 or later)

Newer versions of the HAFM or Element Managers installed on the HAFM appliance automatically download when the remote clients log in to the HAFM appliance.

Installation Procedure

1. Open a Terminal window by choosing **Terminal** from the **Personal Applications** subpanel.
2. At the prompt (#), type `netscape`. Press **Enter**.

   The Netscape browser opens.
3. Type the address of the HAFM appliance in the **Location** (or **Address**) field of the browser, then press **Enter**.

   Obtain the HAFM appliance address from your network administrator

   The **HP StorageWorks HAFM** page displays. Figure 111 illustrates a partial page with the Windows installation section.
4. Read the instructions for your operating system.

   If a reference to fixes is made, click the hyperlink and verify that your system is up-to-date.
5. On the page, click **Begin HP-UX Installation/Begin AIX Installation /Begin Linux Installation** to begin the installation process. If you have read the security agreement information and wish to continue, click **Yes**. The **HP High Availability Fabric Manager Available Installers** page displays, as shown in Figure 112.
6. On the **HP High Availability Fabric Manager Available Installers** page, click **Download**. The File Download dialog box displays, as shown in Figure 113.
7. Click Open. The system begins downloading the HAFM installer. When the download is complete, the **Introduction** screen displays.
8. A **Save As** dialog box displays automatically with the default filename `hpClientInstall.bin`. Change the filename to: `/home/hpClientInstall.bin`. Click **OK**. The software download begins.
9. Close the Netscape window.
10. In the Terminal window, type `cd home`. Press **Enter**. Then type `sh hpClientInstall.bin`. Press **Enter**. When the download is complete, the **Introduction** screen displays.

    Be aware that there may be a considerable delay.
11. Click **Next**. At any time, you may return to the previous page by clicking **Previous** or quit the Installer by clicking **Exit**. The **License Agreement** screen displays.

12. If you have read the license agreement and agree to accept the terms, click **I accept the terms of the License Agreement**.
13. Click **Next**. The **Important Information** screen displays.
14. Click **Next**. The **Choose Install Folder** screen displays.
15. Choose a folder on the remote workstation in which to store the HAFM software. You can accept the default location, type in the path to a new location, or click **Choose** to browse for an appropriate location. Click **Restore Default Location** to change the location back to the default.
16. Click **Next**. The **Choose Shortcut Location** screen displays.

Note: If the HAFM is already installed on the system, you are prompted to uninstall the existing version of the HAFM. If you want to uninstall the existing software, click **Yes** and press **Next**. In the Uninstall High Availability Fabric Manager window, click **Uninstall**. When the uninstall process is done, click **Quit**.

---

17. Select a shortcut location from this screen. The options for the location of HAFM links are:
    - **In your home folder**—Adds a new program group on the **Start** menu for the HAFM.
    - **Other**—Enables you to choose any location on your hard drive or network for the HAFM files.
    - **Don't create links**—Prevents the installation from creating a link for the HAFM.
18. Click **Next** to begin the installation. The **Pre-Installation Summary** screen displays.
19. Review the installation information and click **Install**.

    The progress of the installation is tracked on the **Installing High Availability Fabric Manager** screen.
20. If desired, enable the **Start the High Availability Fabric Manager** check box to immediately open the HAFM. Click **Done** to close the **Install Complete** dialog box.

Running the High Availability Fabric Manager

Run the HAFM program from the directory in which you saved it.

1. In the Terminal window, type:

   ```
   cd HAFM
   ```

2. Press **Enter**.
3. Type:

   ```
   ./HAFM
   ```

4. Press **Enter**. The *HAFM* application opens.

Editing Batch Files

This appendix provides instructions for updating batch files. It includes:

Configuring the Application to Use Dual Network Cards

Issues with client-to-server connectivity can be due to different causes. Some examples are:

- The computer running the application has more than one network card (NIC) installed.
- The computer running the application is behind a firewall that performs network address translation.

In order to ensure that clients can connect to the server, edit the `HAFM_sc.bat` file to manually specify the IP address that the server should communicate to its clients.

Windows Systems

1. Open the `<Install_Home>\bin\HAFM_sc.bat` file using a text editor.
2. Find the following lines and add the bold text with one space before and after the text:

```
rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m
-Xminf.15  -Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/
-Djava.rmi.server.hostname=x.x.x.x -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.flavor=%APP_FLAVOR% Server
```

where **x.x.x.x** is the desired IP address for the appliance

Setting the Zoning Delay

Edit the batch file to set the application to configure zoning through either ECC or Telnet. If a response is not received within the amount of time specified here, the application ends the operation and report that it failed. If the flag is not set, the time-out returns to its default setting of 180000 ms (180 sec).

Note: Setting large zones through Telnet can take a long time for large zone sets—approximately six seconds for each zone set.

Windows Systems

1. Open the `<Install_Home>\bin\HAFM_sc.bat` file using a text editor.
2. Find the following lines and add the bold text with one space before and after the text:

```
rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.flavor=%APP_FLAVOR% Server
```

3. Edit the `-Dsmp.zoning.wait.timeout` entry. Be sure to add a space after your entry.
4. Save and close the file.

Specifying a Host IP Address in Multi-NIC Networks

In a network that has two or more NICs, the local host IP returns one of the IPs known to the system. To specify which IP is returned, edit the `Dsmp.server.edipaddress` variable to instruct the Trap Event Distributor to use a specific IP address.

Windows Systems

1. Open the `<Install_Home>\bin\HAFM_sc.bat` file using a text editor.
2. Edit the following lines:

```
rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.flavor=%APP_FLAVOR% Server
```

   to read:

```
rem HAFM Server

start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -Xincgc -classpath %CLASSPATH% -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/
-Dsmp.server.edipaddress=x,x,x,x -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.flavor=%APP_FLAVOR% Server
```

   where **x.x.x.x** is the desired IP address.

Reference

This appendix provides useful reference information.

Compatibility with Other Applications

The application is designed to operate smoothly with other Enterprise applications and network-monitoring programs. Because this application has fully configurable SNMP trap listening and forwarding functions, it can act as a primary or secondary network manager. It can listen for trap events on any port and can forward traps to other network management software, enabling easy integration into existing systems.

By default, the application is configured to listen for traps on the standard port, 162. Only one software application can control a TCP/IP port at a given time. If the application is not the primary network management tool and you plan to run the application on the same computer, you may need to reconfigure the application to listen for traps on a different port. For instance, if the primary network management software is configured to listen for traps on port 162 and forward them on port 3000, reconfigure the application to listen for traps on port 3000.

Icon Legend

Various icons are used to illustrate devices and connections in a SAN. The following tables list icons that display on the Physical Map.

Product Icons

The following table lists the SAN product icons that display on the topology. Some of the icons shown in Table 22 only display when certain features are licensed. In the case of HP devices, if another appliance is managing a HP device, the Generic HP icon displays.

Table 22: Product Icons

Icon	Description	Icon	Description
	Host Bus Adapter (HBA)		Network Attached Storage (NAS)
	Switch		Storage
	Bridge		Hub
	Unknown		Tape
	FCIP Bridge or Gateway		Loop
	iSCSI Bridge or Gateway		appliance
	HP StorageWorks Edge Switch 2/16		HP StorageWorks Edge Switch 2/32
	HP StorageWorks Edge Switch 2/24		Generic HP StorageWorks Switch or Director
	HP StorageWorks Director 2/64		HP StorageWorks Director 2/140

Product Status Icons

Table 23: Product Status Icons

Icon	Status
No icon	Operational
	Degraded
	Failed
	Unknown/Offline

Event Icons

Table 24: Event Icons

Icon	Description
	Informational
	Warning
	Fatal

Band Information Status Icons

Table 25: Band Information Status Icons

Icon	Out-of-Band	In-Band	Icon	Out-of-Band	In-Band
	Present	Not Present		Present	Present
	Failed	Not Present		Present	Failed
	Not Present	Present		Failed	Present
	Not Present	Failed		Failed	Failed

Planned Device Icons

Icons of planned devices illustrate the device being unpacked from a box. Table 26 illustrates the planned icons for various devices.

Table 26: Planned Device Icons

Icon	Description	Icon	Description
	Planned Host Bus Adapter (HBA)		Planned Network Attached Storage (NAS)
	Planned Switch		Planned Storage
	Planned Hub		Planned Tape
	Planned Bridge		Planned Unknown Device
	Planned JBOD		Planned appliance

Group Icons

Table 27: Group Icons

Icon	Description	Icon	Description
	Host		Isolated Group
	Switch		Bridge
	Loop		Fabric

Connections

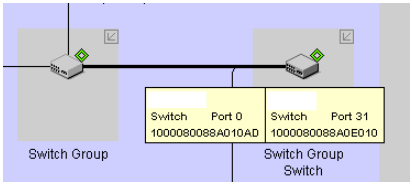


Figure 114: Online connection with online devices

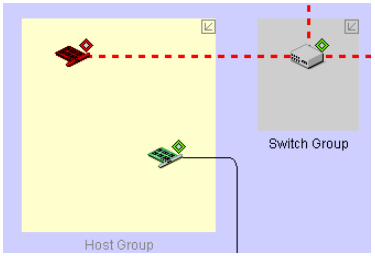


Figure 115: Offline connection and offline loop and storage device

Note: In Figure 116, gray lines on the HBA indicate no activity on those connections.

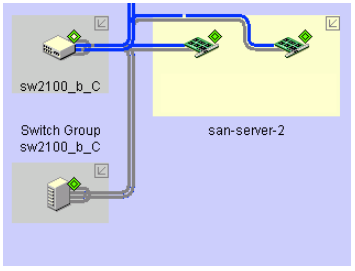


Figure 116: Connection performance as displayed on Physical Map

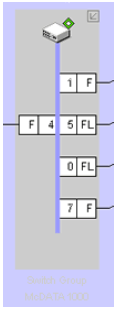


Figure 117: Switch on Topology showing ports

Zoning Naming Conventions

The following naming rules apply for zone names and zone set names:

- Names must begin with alphabetic characters, but may be followed by alphanumeric characters or underscores.
- Names must be unique and are case insensitive.
- Names cannot include spaces.
- Names cannot begin with “SANav_”. This prefix is reserved.
- Character limit: 57 characters.
- No duplicate names are allowed across the zone libraries or between zones and zone sets.

Event Management

Event Management enables you to specify triggers and actions to automate tasks. For example, you can set an event trigger to fire at a certain time and day (everyday at noon) and associate the action of sending an e-mail message.

Event Trigger Properties

Refer to the information in this section for descriptions of the properties you can set for event triggers.

SNMP Trap Event Properties

SNMP trap events occur when the appliance receives an SNMP trap.

Event Property

Table 28: Event Property

Property	Description
IP Address	Device's IP address.
Node Name	Device's world-wide name.
Port Name	Port's world-wide name.
Source	The cause of the event (for example, user ID or device label).
Description	Event description (for example, Out-of-band offline).
Event Level	The severity of the event (for example, informational).

Device Property

The properties of a device in the SAN.

Table 29: Device Property

Property	Description
Label	Device's label, as shown on the Physical Map.
Name	Device's name, as specified in the *Properties* dialog box.
Device Type	Type of device (for example, HBA).
Node Name	Device's world-wide name.
IP Address	Device's IP address.
Vendor	Device's vendor.

Table 29: Device Property (Continued)

Property	Description
Model	Device's model.
Serial Number	Device's serial number.
Port Count	Device's port count.
Firmware	Device's firmware level.
Comments	User-entered comments.
Text1 through Text4	User-entered values.
Device Status	Device's availability (online/offline).

System Property Set

The properties of the operating system and the appliance.

Table 30: System Property Set

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN.
Client Count	Number of clients logged in to the SAN.
Discovery Off	Specifies whether discovery is turned on.
Event Notification Off	Specifies whether event notification is turned on.
Free Memory	Available physical memory.
IP Address	Appliance's IP address.
VM Name	Name of the Java Virtual Machine.
VM Vendor	Vendor of the Java Virtual Machine.
VM Version	Version of the Java Virtual Machine.
OS Architecture	Operating system architecture.
OS Name	Operating system name.
OS Version	Operating system version.
Server Name	Name of the appliance.
Subnet Mask	Discovered subnet mask.
Total Memory	Total physical memory.
Trap Forwarding Off	Specifies whether trap forwarding is enabled.

Table 30: System Property Set (Continued)

Property	Description
Region	The region of the world where the user is located.
Time Zone	User's time zone.
User Count	Number of users.

Performance Event Properties

Performance events occur when the performance at a switch port crosses a user-defined threshold.

Event Property Set

Table 31: Event Property Set

Property	Description
Threshold Type	Performance threshold type (for example, high critical).
Measure Type	Performance measurement units.
Port Number	Port number that encountered an event.
IP Address	IP address of the device that encountered an event.
Source	Label of the device where the event occurred.
Node Name	World-wide name of the device that encountered an event.
Port Name	World-wide name of the port that encountered an event.
Description	Description of the performance event.
Event Level	Severity level.

Device Property Set

The properties of a device in the SAN.

Table 32: Device Property Set

Property	Description
Label	Device's label, as shown on the Physical Map.
Name	Device's name, as specified in the *Properties* dialog box.
Device Type	Type of device (for example, HBA).
Node Name	Device's world-wide name.

Table 32: Device Property Set (Continued)

Property	Description
IP Address	Device's IP address.
Vendor	Device's vendor.
Model	Device's model.
Serial Number	Device's serial number.
Port Count	Device's port count.
Firmware	Device's firmware level.
Comments	User-entered comments.
Text1 through Text4	User-entered values.
Device Status	Device's availability (online/offline).

System Property Set

The properties of the platform and the appliance.

Table 33: System Property Set

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN.
Client Count	Number of clients logged in to the SAN.
Discovery Off	Specifies whether discovery is turned on.
Event Notification Off	Specifies whether event notification is turned on.
Free Memory	Available physical memory.
IP Address	Appliance's IP address.
VM Name	Name of the Java Virtual Machine.
VM Vendor	Vendor of the Java Virtual Machine.
VM Version	Version of the Java Virtual Machine.
OS Architecture	Operating system architecture.
OS Name	Operating system name.
OS Version	Operating system version.
Server Name	Name of the appliance.
Subnet Mask	Discovered subnet mask.
Total Memory	Total physical memory.

Table 33: System Property Set (Continued)

Property	Description
Trap Forwarding Off	Specifies whether trap forwarding is enabled.
Region	The region of the world where the user is located.
Time Zone	User's time zone.
User Count	Number of users.

User Action Event Properties

User action events occur when you change a setting in the appliance.

Event Property Set

Table 34: Event Property Set

Property	Description
Description	Description of the performance event.
Source	User ID of the user who performed the action.
IP Address	IP address of the client from which the action was taken.
Node Name	World-wide name of the device that encountered an event.
Port Name	World-wide name of the port that encountered an event.
Event Level	Severity level of the event (always informational).

System Property Set

The properties about the platform and the appliance.

Table 35: System Property Set

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN.
Client Count	Number of clients logged in to the SAN.
Discovery Off	Specifies whether discovery is turned on.
Event Notification Off	Specifies whether event notification is turned on.
Free Memory	Available physical memory.
IP Address	Appliance's IP address.
VM Name	Name of the Java Virtual Machine.

Table 35: System Property Set (Continued)

Property	Description
VM Vendor	Vendor of the Java Virtual Machine.
VM Version	Version of the Java Virtual Machine.
OS Architecture	Operating system architecture.
OS Name	Operating system name.
OS Version	Operating system version.
Server Name	Name of the appliance.
Subnet Mask	Discovered subnet mask.
Total Memory	Total physical memory.
Trap Forwarding Off	Specifies whether trap forwarding is enabled.
Region	The region of the world where the user is located.
Time Zone	User's time zone.
User Count	Number of users.

User Property Set

The properties of a user.

Table 36: User Property Set

Property	Description
ID	The user ID of the user who performed the action.
Role	The access level of the user who performed the action (for example, Admin or Browse).
Clients For This User	The number of client sessions open for the specified user.

Device State Event Properties

Device state events occur when a device or connection goes online or offline.

Event Property Set

Table 37: Event Property Set

Property	Description
Device Status	Status of the device (online or offline).
Discovery Type	In-band or out-of-band discovery.
Element Type	A device status event or a link status event.
Source	Label of the device that encountered an event.
IP Address	IP address of the device that encountered an event.
Node Name	World-wide name of the device that encountered an event.
Port Name	World-wide name of the port that encountered an event.
Description	Description of the event.
Event Level	Severity level of the event.

Device Property Set

The properties about a device in the SAN.

Table 38: Device Property Set

Property	Description
Label	Device's label, as shown on the Physical Map.
Name	Device's name, as specified in the *Properties* dialog box.
Device Type	Type of device (for example, HBA).
Node Name	Device's world-wide name.
IP Address	Device's IP address.
Vendor	Device's vendor.
Model	Device's model.
Serial Number	Device's serial number.
Port Count	Device's port count.
Firmware	Device's firmware level.
Comments	User-entered comments.
Text1 through Text4	User-entered values.
Device Status	Device's availability (online/offline).

System Property Set

The properties about the platform and the appliance.

Table 39: System Property Set

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN.
Client Count	Number of clients logged in to the SAN.
Discovery Off	Specifies whether discovery is turned on.
Event Notification Off	Specifies whether event notification is turned on.
Free Memory	Available physical memory.
IP Address	Appliance's IP address.
VM Name	Name of the Java Virtual Machine.
VM Vendor	Vendor of the Java Virtual Machine.
VM Version	Version of the Java Virtual Machine.
OS Architecture	Operating system architecture.
OS Name	Operating system name.
OS Version	Operating system version.
Server Name	Name of the appliance.
Subnet Mask	Discovered subnet mask.
Total Memory	Total physical memory.
Trap Forwarding Off	Specifies whether trap forwarding is enabled.
Region	The region of the world where the user is located.
Time Zone	User's time zone.
User Count	Number of users.

Writing Event Management Macros

You can write macros for Event Management to add relevant data to the action phrases. The following actions allow macros:

- email
- Launch
- Log
- Message

When you right-click near the cursor in a text area, a menu of the context property sets displays. Select one of the choices to see a list of the context properties available. Select one of the properties to insert a bracketed macro at the cursor.

When the trigger fires, the values for the context properties that you selected are inserted into the text in place of the macro. Write the text in such a way that you know what the value is since the property name is not inserted along with the value. Example: “The device labeled ${PROPlabel} has come back online. Its Node Name is ${PROPnodename}.

Note: Actions that are triggered by a schedule trigger do not have access to Device and Event properties since no device is directly involved in triggering the policy.

Table 40: Event Context Property Set

Property	Description
Device Status	Status of the device (online or offline).
Discovery Type	In-band or out-of-band discovery.
Element Type	A device status event or a link status event.
Threshold Type	Performance threshold type (for example, high critical).
Measure Type	Performance measurement units.
Port Number	Port number that encountered an event.
IP Address	IP address of the device that encountered an event.
Source	Label of the device that encountered an event.
Node Name	World-wide name of the device that encountered an event.

Table 40: Event Context Property Set

Property	Description
Port Name	World-wide name of the port that encountered an event.
Description	Description of the event.
Event Level	Severity level of the event.

Table 41: Device Context Property Set

Property	Description
Label	Device's label, as shown on the Physical Map.
Name	Device's name, as specified in the *Device Properties* dialog box.
Device Type	Type of device (for example, HBA).
Node Name	Device's world-wide name.
IP Address	Device's IP address.
Vendor	Device's vendor.
Model	Device's model.
Serial Number	Device's serial number.
Port Count	Device's port count.
Firmware	Device's firmware level.
Comments	User-entered comments.
Text1 through Text4	User-entered values.
Device Status	Device's availability (online/offline).

Table 42: TIME Context Property Set

Property	Description
MM:dd:hh:mm:ss	Specifies date and time by month, day, hour, minute, and second.
hh:mm:ss	Specifies the time by hour, minute, and second.
raw	Specifies the time, in milliseconds, since Jan 1, 1970 UTC. For example, 1027966562386.
<User-defined>	This format comes from the Java SimpleDateFormat class. Refer to http://java.sun.com/j2se/1.3/docs/api/ for additional information.

Table 43: User Context Property Set

Property	Description
ID	The ID of the user who performed the action.
Role	The access level of the user who performed the action (for example, Admin or Browse).
Clients For This User	The number of client sessions open for the specified user.

Table 44: System Context Property Set

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN.
Client Count	Number of clients logged in to the SAN.
Discovery Off	Specifies whether discovery is turned on.
Event Notification Off	Specifies whether event notification is turned on.
Free Memory	Available physical memory.
IP Address	Appliance's IP address.
VM Name	Name of the Java Virtual Machine.
VM Vendor	Vendor of the Java Virtual Machine.
VM Version	Version of the Java Virtual Machine.
OS Architecture	Operating system architecture.
OS Name	Operating system name.
OS Version	Operating system version.
Server Name	Name of the appliance.
Subnet Mask	Discovered subnet mask.
Total Memory	Total physical memory.
Trap Forwarding Off	Specifies whether trap forwarding is enabled.
Region	The region of the world where the user is located.
Time Zone	User's time zone.
User Count	Number of users.

- **EXEC Context Property Set**—Executes the command that is contained in the macro, then replaces it with the output of that command.

- **FILE Context Property Set**—Inserts the contents of the file whose path and file name you specify in the macro.

Keyboard Shortcuts

You can use the keystrokes shown in Table 45 to perform common functions.

Note: To open a menu using keystrokes, press **ALT** + the underlined letter. To open a submenu, release the **ALT** key first, then press **SHIFT** + the key for the underlined letter of the submenu option.

Table 45: Keyboard Shortcuts

Menu Item or Function	Keyboard Shortcut
All Panels	F12
Collapse All	CTRL + L
Copy	CTRL + C
Cut	CTRL + X
Delete	Delete
Delete All	CTRL +Delete
Expand All	CTRL + E
Help	F1
Insert Devices	CTRL +D
New Plan	CTRL + N
Open Plan	CTRL + O
Paste	CTRL + V
Product List	F9
Properties	CTRL + P
Master Log	F5
Select All	CTRL + A
Select Connections	CTRL + T
Event Management	F11

Table 45: Keyboard Shortcuts (Continued)

Menu Item or Function	Keyboard Shortcut
View Selected Device's Ports	F4
View Physical Map	F7
View Utilization Connections	CTRL + U

Index

C

D

E

F

G

H

I

R

S

T